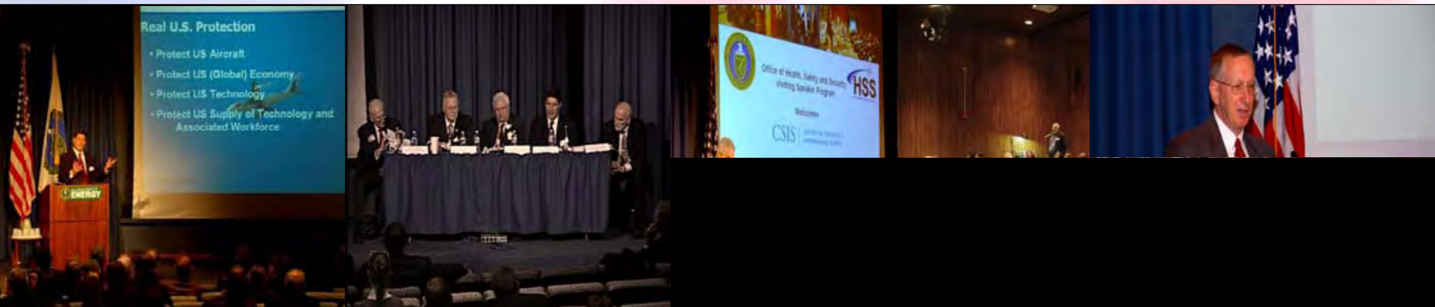
HSS
Office of Health, Safety and Security

Fraud and Theft in the Information Age

Frank W. Abagnale
Author, Lecturer, Consultant

Office of Health, Safety and Security
Visiting Speaker Program Event

October 28, 2009
Washington, DC

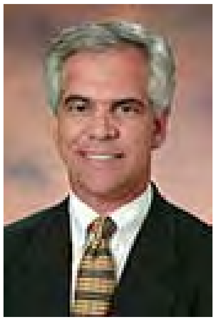

Real U.S. Protection
• Protect US Aircraft
• Protect US (Global) Economy
• Protect US Technology
• Protect US Supply of Technology and Associated Workforce
ENERGY
Office of Health, Safety and Security Visiting Speaker Program
HSS
Welcomes
CSIS

Office of Health, Safety and Security

The Office of Health, Safety and Security (HSS) is the Department of Energy's (DOE) corporate organization responsible for health, safety, environment, and security; providing corporate leadership and strategic vision to coordinate and integrate these vital programs. HSS is responsible for policy development and technical assistance; corporate analysis; corporate safety and security programs; education and training; complex-wide independent oversight; and enforcement. The Chief Health, Safety and Security Officer advises the Secretary and the Deputy Secretary on all matters related to health, safety and security across the complex.

Through its research on sustainability and industry's successful use of its concept, HSS has a clear idea of the types of organizations with which it would be beneficial to collaborate on sustainability. Such outreach efforts provide a cooperative advantage of sustaining an organization's efficiency and vitality by bringing together creative thought and diverse viewpoints toward common goals while demonstrating leadership's commitment to listening to and reflecting the concerns and issues of its shareholders and stakeholders.

As the first phase of its outreach efforts, HSS created a Focus Group forum. The HSS Focus Group forum integrates senior HSS managers from across the organization to discuss and address topics and issues of interest to DOE managers and stakeholders. The objective of the Focus Group is to establish a means for responding to questions and concerns regarding HSS initiatives and activities for improving, the health, safety, and environmental and security performance within the Department and to maintain an ongoing dialogue with involved parties supportive of these efforts. HSS believes an outcome of these continuing discussions and collaborations will be improved worker health and safety programs and the solidification of a safety culture at DOE sites.



Glenn S. Podonsky
Chief Health, Safety and Security Officer

HSS Visiting Speaker Program

The next phase of HSS outreach activities is the creation of the Visiting Speaker Program. The Visiting Speaker Program consists of presentations by leaders drawn from a variety of disciplines to include business, organizational theory, performance management, sustainability, and organizational resilience, made to HSS management and selected attendees from other interested organizations (i.e., Office of Science, Office of Environmental Management, and the National Nuclear Security Administration).

The program is intended to focus agency attention at the management level to the emerging challenges and issues threatening the national security and economic prosperity of the United States. DOE's mission, supported by HSS and other agency organizations, requires the most efficient and resilient leadership and organizational structure for successful mission completion and the continued safety, security, and prosperity of the nation. By inviting and having presenters from the wide range of public and private sector organizations, HSS is encouraging the transformation of government and demonstrating the various stages for change. This includes understanding the depth of the global issues, need for change, tools and means for transformation, and knowing the appropriate performance measurements to determine success and implement evolving management initiatives.

Frank W. Abagnale
Author, Lecturer, and Consultant
Visiting Speaker

Frank W. Abagnale is one of the world's most respected authorities on the subjects of forgery, embezzlement and secure documents. For over thirty years he has lectured to and consulted with hundreds of financial institutions, corporations and government agencies around the world.

Mr. Abagnale has been associated with the FBI for over 35 years. He lectures extensively at the FBI Academy and for the field offices of the Federal Bureau of Investigation. More than 14,000 financial institutions, corporations and law enforcement agencies use his fraud prevention programs. In 1998, he was selected as a distinguished member of "Pinnacle 400" by CNN Financial News. Today Mr. Abagnale is a member of the Board of Editors for Bank Fraud and IT Security, as well as the Financial Fraud Law Report.

Today, the majority of Mr. Abagnale's work is for the U. S. government. His company does not sell products or provide services with the exception of his public speaking engagements which are handled through Keppler Speakers (www.kepplerspeakers.com) in Washington, DC.

Mr. Abagnale does not grant media interviews nor comment on ongoing federal investigations.

Mr. Abagnale believes that punishment for fraud and recovery of stolen funds are so rare, prevention is the only viable course of action.

FRANK W. ABAGNALE
SECURE DOCUMENT CONSULTANT
SINCE 1976

Roland P. Cloutier
Speaker Sponsor
Vice President, Chief Security Officer
EMC Global Security Organization
EMC Corporation

Roland Cloutier is EMC's Vice President & Chief Security Officer, managing EMC's efforts in protecting $22B in assets and nearly $15B in revenue. As EMC's most Senior Security Executive, he is responsible for establishing EMC's brand of trust with its customers and for providing business protection operations worldwide through the management of EMC's innovative converged Global Security Organization. Roland has functional and operational responsibility for all of EMC's information, risk, crisis management, investigative, fraud, and workforce security operations. The GSO's mission is to ensure that EMC all of their brands can continue to develop, build, and deliver the worlds most trusted and leading Information Infrastructure technologies and services securely around the world.

Roland is an industry expert in the development and delivery of Corporate Protection in both the commercial and government sectors. From Critical Infrastructure Protection such as Government, Energy, and Health Services to commercial manufacturing, retail, financial, consumer, and biomedical markets, Roland brings 20 years of experience in security and enforcement program development services and leadership to this field. As an industry innovator, Roland has pioneered corporate protection programs in the areas of Global Growth Security Assurance, Third Party Management, M&A integration, and Applied Converged Security Management.

Prior to EMC, Roland was the Vice President of Cyber Security at AimNet Solutions, a national critical infrastructure consulting and managed services firm where he was responsible for leading AimNet's Cyber Security Services Group, including all aspects of service delivery to Professional Service and Managed Service Security clients. He was selected for that position after serving as the VP of Technology and the National Director for Information Protection at Paradigm Technology Partners which was acquired by AimNet in November of 2003. Roland previously served as the Global Practice Leader in Forensic Services at Global Network Technology Services, a highly specialized systems security, forensics, and investigations firm serving commercial and government clients globally. Prior to his executive position with GNTS, he founded and led Brac Solutions, which was acquired by GNTS, a Cabletron Company.

Roland’s international business security services experience began while serving as an Information Assurance Engineer Manager for EDS of Plano, Texas, where he designed and implemented systems security teams for EDS’s international clients. His global law enforcement and protection experience is derived from more than nine years in federal law enforcement. After serving in the United States Air Force as a Police Officer, including in the Persian Gulf War, he joined the Department of Defense Police & Security Services as an Aerospace Protection Specialist in domestic and international field operations and later served as a Detective with the Untied States Department of Veterans Affairs including an assignment to the State Department for Olympic Security Operations in 1996.

Roland is an innovative force in the industry as a participating member of the Security for Business Innovation Council, the Center for Information Policy Leadership in Washington, D.C., and the Information Technology Sector Coordinating Council in Washington, D.C. Roland is a CISSP, Microsoft Certified Systems Engineer and Internet Specialist, a Certified Checkpoint Systems Engineer, a member of the High Tech Crime Investigations Association, the U.S. State Department Partnership for Critical Infrastructure Security, the National Domestic Preparedness Homeland Security Task Force, and a member of the Infraguard Program of the Federal Bureau of Investigation. Roland’s education includes studies in Criminal Justice and Information Technology at Boston University, Holyoke College, and Community College Of The Air Force.

EMC^2

where information lives

U.S. Department of Energy
Washington, D.C.

ORDER

DOE O 206.1

Approved: 1-16-09

SUBJECT: DEPARTMENT OF ENERGY PRIVACY PROGRAM

1. PURPOSE.

   a. Ensure compliance with privacy requirements, specifically those provided in the Privacy Act of 1974, as amended at Title 5 United States Code (U.S.C.) 552a, Section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB) directives.

   b. Establish a Departmental training and awareness program for all DOE Federal and contractor employees to ensure personnel are cognizant of their responsibilities for—

      (1) safeguarding Personally Identifiable Information (PII) and

      (2) complying with the Privacy Act.

   c. Provide Departmental oversight to ensure compliance with Federal statutes, regulations and Departmental Directives related to privacy.

2. CANCELLATION. DOE N 206.5, *Response and Notification Procedures for Data Breaches Involving Personally Identifiable Information*, dated 10-09-07, is canceled. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual obligation to comply with the directive. Contractor requirement documents (CRDs) that have been incorporated into or attached to a contract remain in effect until the contract is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.

   a. DOE Elements. Except for the exclusions in paragraph 3c, this Order applies to all Departmental Elements, including those created after the Order is issued. (Go to www.directives.doe.gov/pdfs/reftools/org-list.pdf for the current listing of Departmental Elements.)

      The Administrator of the National Nuclear Security Administration (NNSA) will ensure that NNSA employees and contractors comply with their respective responsibilities under this Order.

   b. DOE Contractors. Except for the exclusions in paragraph 3c, the CRD (Attachment 1) sets forth contractor requirements. The CRD will apply to the extent set forth in each contract.

   c. Exclusions. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 USC sections 2406 and 2511, and to ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.

4. REQUIREMENTS. The following privacy requirements apply to all Departmental Elements.

a. Safeguarding Personally Identifiable Information (PII).

(1) OMB has defined PII as any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.

(2) Employees are required to prevent the unauthorized breach of PII.

(3) Upon a finding of a suspected or confirmed data breach involving PII in printed or electronic form, DOE employees must immediately report the incident to the DOE-Cyber Incident Response Capability (DOE-CIRC) at 866-941-2472 (doecirc@doecirc.energy.gov) and through their Departmental Element in accordance with existing cyber incident reporting processes, which have been established in Senior DOE Management Program Cyber Security Plans (PCSPs) as defined in DOE O 205.1A, *Department of Energy Cyber Security Management*.

(4) Types of breaches that must be reported include, but are not limited to the following:

(a) loss of control of DOE employee information consisting of names and Social Security numbers,

(b) loss of control of Department credit card holder information,

(c) loss of control of PII pertaining to the public,

(d) loss of control of security information (e.g., logons, passwords, etc.),

(e) incorrect delivery of PII,

(f) theft of PII, and

(g) unauthorized access to PII stored on Department-operated web sites.

(5) Within one hour of receiving the report of an incident involving a breach of PII, the Office of the Chief Information Officer (OCIO) will report the incident to the United States Computer Emergency Response Team (US-CERT) in accordance with OMB directives. The OCIO will ensure the Chief Privacy Officer (CPO) is notified of all incidents involving the breach of PII within one hour of receiving notification.

(6) PII, regardless of whether it is in paper or electronic form, must be protected from unauthorized access or disclosure throughout its lifecycle.

(7) DOE employees shall limit the use of PII to only that information which is specifically needed to carry out their duties.

b. The Privacy Act.

(1) The Privacy Act governs a Federal agency's ability to maintain, collect, use, or disseminate a record about an individual.

(2) Any grouping of information about an individual that is maintained by an agency, including, but not limited to, his or her education, financial transactions, medical history, and criminal or employment history and that contains his or her name or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph is considered a record for the purposes of the Privacy Act.

(3) The Privacy Act allows an agency to maintain information about an individual that is relevant and necessary to the purpose of the agency as required by statute or by Executive Order of the President.

(4) Information collected under the Privacy Act must be stored in a Privacy Act System of Records (SOR).

(5) A SOR has the following two key distinctions:

(a) an indexing or retrieval capability built into the system and

(b) the Department retrieves records about individuals by reference to a personal identifier, such as the individual's name or Social Security number.

(6) The Privacy Act requires agencies to publish a System of Records Notice (SORN) in the Federal Register and report to Congress when a new SOR

is proposed or significant changes are made to a previously established system.

(7) Each SORN must contain the following information:

(a) name and location of the system;

(b) categories of individuals on whom records are maintained in the system;

(c) categories of records maintained in the system;

(d) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

(e) policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(f) title and business address of the agency official who is responsible for SOR;

(g) agency procedures whereby an individual can be notified at the individual's request if the SOR contains a record pertaining to the individual; and

(h) agency procedures whereby an individual can be notified at the individual's request how he/she can gain access to any record pertaining to him/her contained in the SOR, and how he/she can contest its content; and categories of sources of records in the system.

(8) Under the Privacy Act, with limited exceptions, no agency or person shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

(9) For each SOR, DOE must not permit information collected about an individual for one purpose to be used for another purpose without giving notice to or getting the consent of the subject of the record and unless the record is being used subject to a routine use.

(10) Non-compliance with the Privacy Act carries **criminal and civil** penalties. An employee may be liable if he or she knowingly and willfully—

(a) obtains or requests records under false pretenses,

(b) discloses privacy data to any person not entitled to access, or

(c) maintains a "system of records" without meeting Federal Register notice requirements.

c. Recognizing differences between PII and the Privacy Act and the different obligations created by both authorities. Most personal information about an individual will fall under both the Privacy Act and OMB directives governing the safeguarding of PII. However, employees must be cognizant that these are two separate authorities that impose different responsibilities on federal and contractor employees for safeguarding information. PII that is in a SOR is subject to the restrictions and penalties of the Privacy Act.

d. DOE employees must receive yearly training on privacy and data protection policies.

e. Privacy Impact Assessment. All unclassified information systems shall have a Privacy Impact Assessment (PIA) approved by the Senior Agency Official for Privacy (SAOP) or designated official. PIAs must be reviewed and updated at least annually (see Appendix A).

f. Collection and use of Social Security numbers. Collection and use of Social Security numbers not required by statute, regulation or an intended Departmental purpose shall be eliminated, in practice and in form, from DOE information systems and programs, whether in electronic or paper media.

g. Senior DOE Management, as defined in DOE O 205.1A, *Department of Energy Cyber Security Management*, dated 12-4-06, may add to these requirements for their own organizations, based on assessment of risk, so long as any additional direction is consistent with these requirements.

5. RESPONSIBILITIES.

a. Senior Agency Official for Privacy. Oversees, coordinates, and facilitates the Department's compliance with authorities governing privacy protection.

b. Director, Office of Information Resources. Appoints the Chief Privacy Officer.

c. Chief Privacy Officer.

(1) Manages the Department's Privacy Program.

(2) Reviews Department's PIAs.

(3) Advises and provides subject matter expertise to the Director, Office of Information Resources in the promulgation of guidance on privacy.

(4) Coordinates with the Chief Information Officer (CIO); the Chief Health, Safety and Security Officer; General Counsel (GC); and Heads of Departmental Elements to ensure compliance with the requirements of this Order.

d. Secretarial Officers/Heads of Departmental Elements.

(1) Have responsibility and accountability for ensuring the Departmental Elements' implementation of privacy protections in accordance with Federal laws, regulations, Departmental policies and Directives.

(2) Ensure completion of Privacy Impact Assessments (PIAs) of all unclassified information systems within their purview, including systems that only collect or maintain information about DOE employees and DOE contractors, in accordance with the requirements of this Order and all appendices.

(3) At a minimum, Departmental Elements must implement the following safeguards:

(a) Implement Cyber Security Controls outlined in DOE Directives and Office of the Chief Information Officer (OCIO) guidance for the protection of PII.

(b) Ensure all individuals with authorized access to PII and their supervisors sign at least annually a document clearly describing their responsibilities.

(c) Ensure personnel minimize the collection of PII to only that which is required to conduct business operations necessary for the proper performance of a documented DOE function.

(d) Identify systems that process PII and ensure access is limited to only those individuals whose work requires access.

(e) Use sealable, opaque envelopes for mailing PII. Mark envelope to the person's attention.

(4) Post privacy policy statements on DOE websites in accordance with Federal law, regulations, and OMB directives.

(5) Appoint site Privacy Act Officers or points of contact for their Departmental Elements.

(6) Implement their Elements' plans to eliminate the unnecessary collection and use of Social Security numbers.

e. Chief Information Officer.

(1) Advises and provides cyber security and information technology subject matter expertise to the CPO to identify ways in which the Department can safeguard privacy information.

(2) Provides current threat information regarding the compromise of PII and information systems containing PII.

(3) Reports incidents involving breaches of PII to the United States Computer Emergency Response Team (US-CERT) in accordance with OMB directives and ensures the CPO is notified of all incidents involving the breach of PII within one hour of receiving notification.

f. Privacy Incident Response Team (PIRT).

(1) Convened by the SAOP.

(2) Responds to major incidents involving the breach of PII as determined by the SAOP.

(3) Conducts assessments of incidents involving breaches of privacy data, including evaluating the scope, degree of compromise, impact and risks resulting from the breach.

(4) Coordinates with the SAOP for internal and external agency notification including law enforcement.

g. Privacy Act Officers.

(1) Advocate and promote Privacy program activities within their Departmental Elements.

(2) Advise and provide Privacy Act subject matter expertise to their Departmental Elements, specifically with regard to conducting PIAs and completing the SORN process.

(3) Facilitate compliance reporting for their Departmental Elements.

(4) Manage the process for resolving privacy complaints for their Departmental Elements, including—

(a) documentation of factual circumstances surrounding unresolved complaints and

(b) notifying the CPO of unresolved written complaints.

h. Contracting Officers.

(1) Once notified by the affected Heads of Departmental Elements or their senior level designees regarding which contracts are subject to this Order, incorporate the CRD into affected contracts as directed.

(2) Ensure that contracting officers' representatives (CORs) and/or contracting officers' technical representatives (COTRs) are aware of provisions within this Order and any changes to their respective contracts.

(3) Ensure Privacy Act clauses contained in Federal Acquisition Regulations at 52.224-1 and 52.224-2 are included in all solicitations and in any awarded contracts.

i. DOE Employees.

(1) Are responsible for safeguarding PII and for reporting suspected or confirmed incidents involving the breach of PII, in printed or electronic form, in accordance with the requirements provided in Appendix B.

(2) Are responsible for complying with the Privacy Act.

j. System Owners.

(1) System Owners are Departmental Element officials responsible for monitoring the information systems under their purview to ensure compliance with this Order. System Owners are responsible for the overall procurement, development, integration, maintenance, secure operation, and safeguarding of Privacy information including PII for their information system(s).

(2) System Owners must file a SORN, if applicable, and must complete the entire Federal Register review period before the system will be permitted to operate in the production environment.

(3) System Owners must submit documentation in support of a new or revised SOR or significant alteration to an existing SOR to the CPO. All privacy documentation must be in electronic format and submitted via e-mail to privacy@hq.doe.gov. The CPO, in consultation with General Counsel, will post a SORN in the Federal Register providing interested persons the opportunity to comment on the SOR.

(4) System Owners must submit documentation to the CPO in sufficient time for the CPO, in consultation with GC, to review prior to placing a SOR in operation.

(5) For each SOR a System Owner maintains, the System Owner must—

(a) Maintain only personal information considered relevant and necessary for the legally valid purpose for which it is obtained;

(b) Where possible, collect information directly from the individual;

(c) Prepare documentation for the publication of notice in the Federal Register, when a SOR is established or revised;

(d) Update SORNs prior to any significant change occurring to a System that affects the privacy information kept in the System;

(e) Maintain records with accuracy, relevance, timeliness, and completeness to ensure fairness to the individual of record;

(f) Employ appropriate security controls for the system to protect confidentiality, integrity, and available of records; and

(g) Require persons involved in the design, development, operation, or maintenance of any SOR, or in maintaining any record to sign a Rules of Behavior for each SOR to which they are granted access.

k. General Counsel.

(1) Provides legal review and concurrence before publishing any Departmental SORN in the Federal Register.

(2) Provides legal expertise to all DOE elements in interpreting and applying privacy issues including privacy law, compliance, and training.

6. REFERENCES.

a. Federal Laws and Regulations.

(1) Privacy Act of 1974, as amended at 5 U.S.C. §552a, P.L. 93-579.

(2) E-Government Act of 2002, P.L. 107-347.

(3) Paperwork Reduction Act of 1995, 44 U.S.C. 3501 *et seq*.

(4) DOE Privacy Act Regulation, 10 CFR Part 1008.

(5) The Freedom of Information Act (FOIA), 5 U.S.C. §552.

(6) DOE Regulations Implementing the FOIA, 10 CFR Part 1004.

b. Office of Management and Budget Circulars and Memoranda.

(1) OMB Circular A-130, Management of Federal Information Resources.

(2) OMB Memorandum (M) 99-05, Privacy and Personal Information in Federal Records.

(3) OMB M-99-18, Privacy Policies on Federal Web Sites.

(4) OMB M-00-13, Privacy Policy and Data Collection on Federal Web Sites.

(5) OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

(6) OMB M-05-08, Designation of Senior Officials for Privacy.

(7) OMB M-06-15, Safeguarding Personally Identifiable Information.

(8) OMB M-06-16, Protection of Sensitive Agency Information.

(9) OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments.

(10) OMB M-07-16, Safeguarding Against and Responding to Breaches of Personally Identifiable Information.

c. Department of Energy Directives.

(1) DOE P 205.1, *Departmental Cyber Security Management Policy*, dated 5-8-01.

(2) DOE O 205.1A, *Department of Energy Cyber Security Management*, dated 12-4-06.

(3) DOE N 221.14, *Reporting Fraud, Waste, and Abuse*, dated 12-20-07.

(4) DOE O 221.1A, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*, dated 4-19-08.

(5) DOE O 221.2A, *Cooperation with the Office of Inspector General*, dated 2-25-08.

7. DEFINITIONS.

a. Accuracy. Ensuring, within sufficient tolerance for error, the quality of the record in terms of its use in making a determination.

b. Availability. Ensuring timely and reliable access to and use of information or an information system. For example, a loss of availability is the disruption of access to or use of information or an information system.

c. Breach. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users—and for other than an authorized purpose—have access to or potential access to PII, whether in physical or electronic form.

d. Confidentiality. Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

e. Data Breach Analysis (for incidents involving the breach of PII). The process of assessing what, if any, Privacy information was compromised, the significance of such losses or intrusions, and how to prevent future occurrences.

f. Identity Theft. Per section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a), "a fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation."

g. Information in Identifiable Form. Information in an IT system or online collection: (1) that directly identifies an individual (e.g., name, address, Social Security number or other identifying number or code, telephone number, email address, etc.) or (2) by which an agency intends to identify specific individuals in conjunction with other data elements (i.e. indirect identification). These data elements may include a combination of gender, race, birth date, geographic indicator and other descriptors.

h. Information Technology (IT). As defined in the Clinger-Cohen Act, Pub. L. No. 104-106, IT refers to any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

i. Information System. A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

j. Integrity. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

k. Major Information System. An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

l. National Security System. Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function, operation, or use of which—

(1) involves intelligence activities;

(2) involves cryptologic activities related to national security;

(3) involves command and control of military forces;

(4) involves equipment that is an integral part of a weapon or weapons system;

(5) is critical to the direct fulfillment of military or intelligence missions, not including systems that are to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or

(6) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

m. Necessary. A threshold of need for an element of information greater than mere relevance and utility. A Federal agency should maintain in its records only such information about an individual as is relevant and reasonably necessary to ensure fairness to the individual and to accomplish a purpose of the agency that is required by statute or by Executive Order.

n. Personally Identifiable Information (PII). Any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.

o. Personal Identifier. An identifier such as a Social Security number, fingerprint, name, etc. that uniquely identifies an individual.

p. Privacy Act Information. Information that is required to be protected under the Privacy Act of 1974.

q. Privacy Act Request. A request to an agency to gain access to an individual's record, such as by another Federal agency or law enforcement as required by statute; a request by any individual to gain access to his/her record or to any information pertaining to him/her which is contained in the system.

r. Privacy Impact Assessment (PIA). An analysis of how information is handled to—

(1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

(2) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and

(3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

s. Record. Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

t. Relevance. A limitation to only those elements of information that clearly bear on the determination(s) for which the records are intended.

u. Routine Use. With respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

v. System of Records. A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

w. System of Records Notice (SORN). Notice published in the Federal Register prior to an agency's collection, maintenance, use or dissemination of information about an individual.

x. Timeliness. Sufficiently current to ensure that any determination based on the record will be complete, accurate and fair.

8. NECESSITY FINDING STATEMENT. In compliance with Sec. 3174 of P.L. 104-201 (50 U.S.C. 2584 note), DOE hereby finds that this Order is necessary for the fulfillment of current legal requirements and conduct of critical administrative functions.

9. CONTACT. Questions concerning this Order should be addressed to the Chief Privacy Officer (202) 586-0483.

BY ORDER OF THE SECRETARY OF ENERGY:

JEFFREY F. KUPFER
Acting Deputy Secretary

APPENDIX A. PRIVACY IMPACT ASSESSMENTS

Why are DOE organizations required to conduct PIAs?

The E-Government Act of 2002 requires Federal agencies to perform Privacy Impact Assessments (PIAs), an analysis of how information is handled, in order: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The DOE PIA process helps to ensure privacy protections are considered and implemented throughout the system life cycle.

Step 1 – The Privacy Needs Assessment

System Owners are required to complete the first step of the DOE PIA for all unclassified information systems including contractor systems operated for or on behalf of the agency. This first step of the DOE PIA process is the Privacy Needs Assessment (PNA). The PNA is designed to ensure privacy is addressed for all information systems in an efficient manner by asking four threshold questions:

1. Does the information system collect or maintain information about individuals?

2. Is the information in identifiable form?

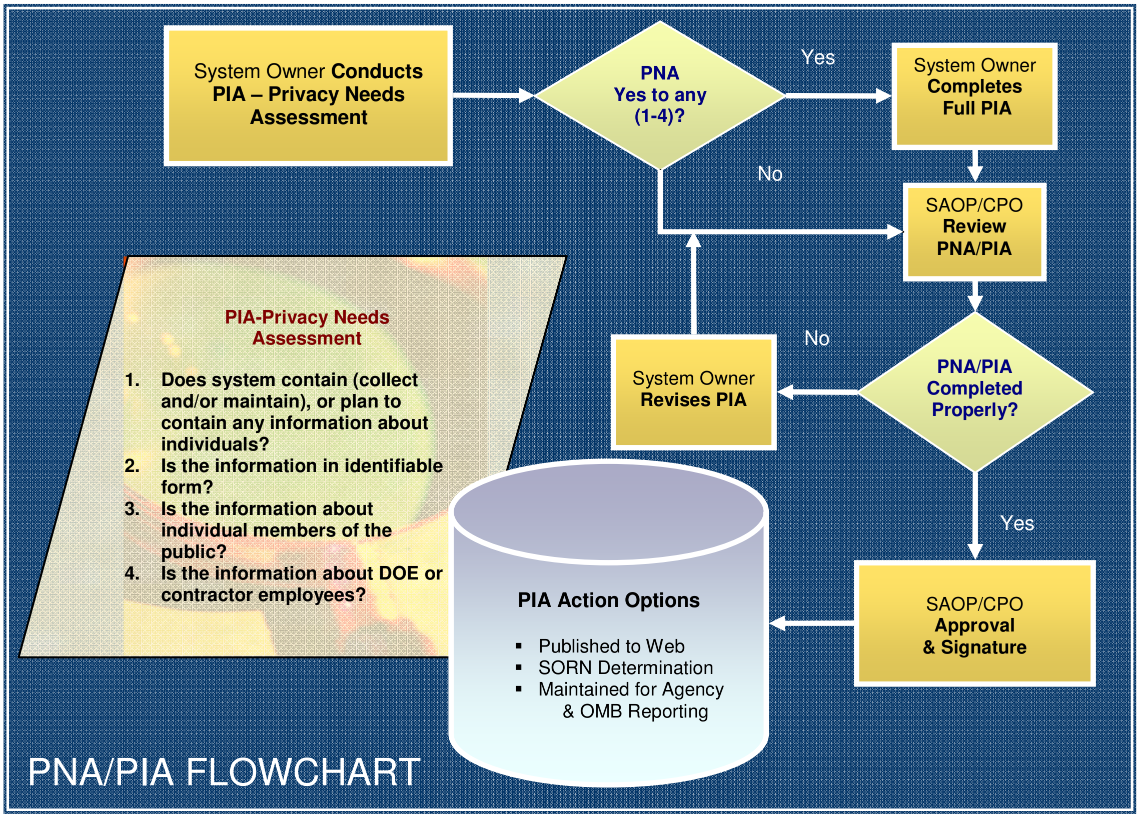
3. Is the information about individual members of the public?

4. Is the information about DOE or contractor employees?

If the answer to any of these questions is “Yes,” System Owners must complete a full PIA.

If the answer to <u>all</u> the threshold questions in the PNA is “No,” no further sections of the PIA must be completed. The System Owner signs the PIA certifying to the CPO that the system does not contain PII.

System Owners and their Privacy Act Officers must sign the PNA and submit the PNA to the DOE CPO. The PNA/PIA Flowchart illustrates this process.


System Owner Conducts PIA – Privacy Needs Assessment
PNA Yes to any (1-4)?
Yes
System Owner Completes Full PIA
No
SAOP/CPO Review PNA/PIA
No
System Owner Revises PIA
PNA/PIA Completed Properly?
Yes
SAOP/CPO Approval & Signature
PNA/PIA FLOWCHART

PIA-Privacy Needs Assessment

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?
2. Is the information in identifiable form?
3. Is the information about individual members of the public?
4. Is the information about DOE or contractor employees?

PIA Action Options

- Published to Web
- SORN Determination
- Maintained for Agency & OMB Reporting

If the answer to any of the questions in the PNA is "Yes" and a full PIA is required, the System Owner, in collaboration with the Privacy Act Officer must—

- Complete applicable elements of the PIA and
- Sign and submit the PIA to the CPO, copying the Head of the Departmental Element (HDE) staff.

If there are issues with the submitted PIA that need to be addressed, the CPO will coordinate with the System Owner to ensure there is an understanding of any deficiencies in the PIA so corrective action may be taken. The SAOP approves and signs the PIA. The CPO provides a signed copy of the PIA to the System Owner. PIAs affecting members of the public will be posted to the DOE Privacy Website in accordance with applicable laws and regulations. The System Owner may also be required to publish a System of Records Notice in the Federal Register.

When to Conduct a Privacy Impact Assessment

Privacy, like security, should be considered at all stages of the system's lifecycle. Departmental Elements must also consider the information lifecycle (i.e. collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect an individual's privacy. PIAs should be conducted as part of the certification and accreditation process. At a minimum, PIAs must be conducted when—

1. Designing, developing or procuring information systems or IT projects that collect, maintain or disseminate information in identifiable form.

2. Initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons.

3. Significantly modifying an information system.

PIAs should be updated whenever there is a change to the information system that affects privacy or creates new risks to privacy. Examples of these changes include the following:

- **Conversions** - when converting paper-based records to electronic systems.

- **Anonymous to Non-Anonymous** - when functions applied to an existing information collection change anonymous information into information in identifiable form.

- **Significant System Management Changes** - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system.

- **Significant Merging** - when organizations adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated.

- **New Public Access** - when authentication technology (e.g., password, digital certificate, biometric) is newly applied to an information system accessed by members of the public.

- **Commercial Sources** - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources (merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement).

- **New Interagency Uses** - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA.

- **Internal Flow or Collection** - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form.

- **Alteration in Character of Data** - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

- **Changed Authorities or Business Processes -** when there are changes in information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form.

Who Completes the Privacy Impact Assessment?

The PIA is the System Owner's responsibility. The System Owner, system developer, data owners and the Privacy Act Officer must work together to complete the PIA.

System Owners must identify data that is collected and maintained in the information system, as well as individuals who will access that data. The Privacy Act Officer must assess whether there are any threats to privacy. PIAs require collaboration with program experts as well as experts in the areas of information technology, cyber security, records management and privacy.

Privacy Impact Assessment Document Review and Approval Process

The completed PIAs must be submitted to the CPO, copying the Heads of Departmental Elements' staff. The CPO submits the PIAs to the SAOP for approval and signature.

If the Chief Privacy Officer indicates corrective action is necessary for a PIA, the PIA will be returned to the System Owner. The System Owner is responsible for identifying and implementing corrective actions prior to resubmitting the PIA to the CPO.

Steps for Completing the DOE Privacy Impact Assessment

Step	Responsible Individual(s)	Actions
1	**System Owner**	**PIA Template** Obtain current DOE PIA template from the Privacy Website. The System Owner has the overall responsibility and accountability for completing the PIA. Privacy should be considered at all stages of the system lifecycle. At a minimum, the PIA should be conducted as part of the certification and accreditation of the system and reviewed at least annually.
2	**System Owner** **Privacy Act Officer**	**Complete PNA portion of the PIA** A. If the answer to all questions on the PNA section of the PIA is "No," the System Owner and Privacy Act Officer must sign and submit the PNA to the CPO, copying the HDE staff. Upon receiving the approval of the SAOP, the PIA is now complete. B. If the answer to any of the questions on PNA is "Yes," proceed to step 3.
3	**System Owner** ▪ Privacy Act Officer ▪ System Administrators ▪ Data Owners ▪ Program Managers ▪ Subject Matter Experts ▪ Information System Security Officer ▪ Security: Cyber & Physical Security ▪ Operations	**Conduct Full PIA** Complete full PIA using DOE PIA template. The template is available from the Privacy Website, and may not be modified. System Owners and Privacy Act Officers must Sign the PIA.
4	**System Owner** **DOE CPO** **DOE CIO**	**Submit PIA to CPO** System Owner submits PIA to CPO for review. The CPO may consult with subject matter experts and GC. If there are any issues with the PIA, the CPO will coordinate with the System Owner to ensure deficiencies are identified. The System Owner corrects deficiencies and resubmits the PIA. Depending on the scope and number of deficiencies, the System Owner may develop a plan of action and milestones for correcting the PIA. Once all deficiencies and concerns have been addressed, the System Owner resubmits the PIA to the DOE CPO.
5	**DOE CPO** **SAOP**	**DOE CPO Submits to SAOP** Having reviewed the PIA, the CPO submits the PIA to the SAOP for signature.
6	**SAOP** **DOE CPO** **System Owner**	**SAOP Signature and Approval** The SAOP approves and signs the PIA. Copies of the signed PIA are maintained with the CPO and provided to the System

Step	Responsible Individual(s)	Actions
		Owner for their records. The System Owner should maintain these records for conducting certification and accreditation and for preparing OMB Exhibits 300 and 53.
7	**SAOP** **CPO** **General Counsel** **System Owner** **Privacy Act Officer**	**System Requires Web Posting and Reporting** If the PIA identifies the system as a system affecting members of the public in accordance with the E-Government Act, the following actions are taken: ▪ CPO posts the signed PIA affecting members of the public to the DOE Privacy website; ▪ Publishes System of Records Notice in the Federal Register, if applicable; ▪ Reports PIAs affecting members of the public to OMB. NOTE: Not all PIAs require a SORN; therefore, there will not be a one-to-one (1:1) ratio of PIAs to SORNs.
8	**System Owner** **Privacy Act Officer**	**Ongoing Monitoring** The System Owner and local Privacy Act Officer will ensure the PIA is reviewed at least annually or whenever there is a change to the system that would impact the risk to privacy. If required, the PIA is updated.

Department of Energy
Privacy Impact Assessment Privacy Needs Assessment

<SAMPLE ONLY>		
Date		
Departmental Element		
Name of Information System or IT Project		
Exhibit Project UID		
	Name, Title	Contact Information Phone, Email
System Owner		
Privacy Act Officer		
Purpose of Information System or IT Project		
Type of Information Contained (Collected or Maintained) Use NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, for guidance.		
Has there been any attempt to verify Information in Identifiable Form does not exist on the system (e.g., system scan)?		
If "Yes," what method was used to verify the system did not contain Information in Identifiable Form?		
Threshold Questions		
1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?		
2. Is the information in identifiable form?		
3. Is the information about individual members of the public?		
4. Is the information about DOE or contractor employees?		
If the answer to the **all** four (4) key threshold questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.		

APPENDIX B. RESPONSE AND NOTIFICATION PROCEDURES FOR DATA BREACHES INVOLVING PERSONALLY IDENTIFIABLE INFORMATION

The purpose of this appendix is to define notification requirements and procedures for incidents involving breaches of PII.

REQUIREMENTS.

Identifying and Reporting Incidents Involving Breaches of PII

1. Upon a finding of a suspected or confirmed data breach involving PII in printed or electronic form, DOE employees will immediately report the incident to the DOE-Cyber Incident Response Capability (DOE-CIRC) at 866-941-2472 (doecirc@doecirc.energy.gov) and through their Departmental Element in accordance with existing cyber incident reporting processes, which have been established in Senior DOE Management Program Cyber Security Plans (PCSPs) as defined in to DOE O 205.1A, *Department of Energy Cyber Security Management*.

2. Types of breaches that must be reported include, but are not limited to the following:

   a. loss of control of DOE employee information consisting of names and Social Security numbers;

   b. loss of control of Department credit card holder information;

   c. loss of control of PII pertaining to the public;

   d. loss of control of security information (e.g., logons, passwords, etc.);

   e. incorrect delivery of sensitive PII;

   f. theft of PII; and

   g. unauthorized access to PII stored on Department operated web sites.

3. Within one hour of receiving the report of an incident involving a breach of PII, the Office of the Chief Information Officer (OCIO) will report the incident to the United States Computer Emergency Response Team (US-CERT) in accordance with OMB directives. The OCIO will ensure the CPO is notified of all incidents involving the breach of PII within one hour of receiving notification.

4. Additionally, the Senior Agency Official for Privacy may convene the Privacy Incident Response Team (PIRT) chaired by the Senior Agency Official for Privacy, and comprised of senior-level representatives from the Offices of the Chief Information Officer; Public Affairs; General Counsel; Office of Management; Office of Health, Safety and Security; National Nuclear Security Administration; and the DOE Program Offices impacted by a PII breach when the PII breach is significant, crosses DOE organizational boundaries, or as needed. The PIRT will coordinate with the Office of

Inspector General (IG) to ensure significant PII breaches involving alleged or suspected crimes are reviewed for potential IG investigation

The following considerations will apply in determining the impact of a PII breach resulting in lost, stolen or improperly accessed data:

a. the nature and content of the data (e.g., the data elements involved, such as name, Social Security number and/or date of birth, etc.);

b. the ability of an unauthorized party to use the data, either by itself or in conjunction with other data or applications generally available, to commit identity theft or otherwise misuse the data to the disadvantage of the record subjects;

c. ease of logical data access to the data given the degree of protection for the data (e.g., unencrypted, plain text, etc.);

d. ease of physical access to the data (e.g., the degree to which the data is readily available to unauthorized access);

e. evidence indicating that the data may have been the target of unlawful acquisition;

f. evidence that the same or similar data had been acquired from other sources improperly and used for identity theft;

g. whether notification to affected individuals through the most expeditious means available is warranted; and

h. whether further review and identification of systematic vulnerabilities or weaknesses and preventive measures are warranted.

5. Upon conclusion of any risk analysis by the party leading the investigative effort (i.e. respective Under Secretary, his or her designees, or the PIRT), if there is a finding of reasonable risk for potential misuse of any PII involved, that information along with any supporting material will be shared with both the Senior Agency Official for Privacy and the Chief Information Officer.

6. If the Senior Agency Official for Privacy and the Chief Information Officer concur that the data breach does not pose a reasonable risk of harm, the Department will take no further action.

7. Conversely, if there is no concurrence, both parties will present their views to the Deputy Secretary, who will then decide what, if any, further action is necessary.

8. The Senior Agency Official for Privacy may provide notice to subjects of a data breach and/or offer them Credit Protection Services prior to the completion of any risk analysis. This decision will likely hinge upon the information available to the Department at the

time of the data breach, and whether the information suggests there is an immediate and substantial risk of identity theft or other harm.

9. The Head of the Departmental Element in which the breach occurred will provide notification to the affected individuals once there is a finding by the PIRT that a reasonable risk exists for potential misuse of any sensitive personal information involved in the data breach. The notification will be signed, and include the following elements as appropriate:

   a. a brief description of what happened, including the dates of the data breach and of its discovery, if known;

   b. to the extent possible, a description of the personnel information that was involved (e.g., full name, Social Security number, date of birth, home address, account numbers, etc.);

   c. a brief description of actions taken by the Department to investigate, mitigate losses and protect against any further breach of data;

   d. contact procedures to ask further questions or learn additional information, including a toll-free telephone number, email address, web site, and/or postal address;

   e. steps that individuals should take to protect themselves from the risk of identity theft, including steps to obtain fraud alerts, if appropriate, and instructions for obtaining other credit protection services (NOTE: Alerts may include key changes to fraud reports and on-demand personal access to credit reports and scores); and

   f. a statement of whether the information was encrypted or protected by other means, when it is determined such information would be beneficial and would not compromise the security of any Departmental systems.

10. When there is insufficient or inaccurate contact information that precludes written notification to an affected individual, an alternative form of written notice may be provided.

   a. This alternative notice may include a conspicuous posting on the home page of the Department's web site and notification in major print and broadcast media, including major media in geographic areas where the affected individuals are likely to reside.

   b. The media notice will include a toll-free telephone number for an individual to contact in order to learn whether or not his/her personal information is possibly included in the data breach.

11. When the SAOP determines that urgent action is required because of possible imminent misuse of PII, the SAOP may provide information to affected individuals by telephone or other means, as appropriate.

12. Notwithstanding the foregoing requirements, notification may be delayed upon lawful requests to protect data or computer resources from further compromise or to prevent interference with the conduct of lawful investigation, national security, or efforts to recover data.

    a. A lawful request should be made in writing to the Secretary of Energy or SAOP by the Federal agency responsible for the investigation regarding security concerns or data recovery efforts that may be adversely affected by providing notification.

    b. The SAOP must be notified of a delay notification request.

    c. Any lawful request for delay in notification must state an estimated timeframe after which the requesting entity believes that notification will not adversely affect the conduct of the investigation or efforts to recover data.

    d. Any delay should not increase risk or harm to any affected individuals.

    e. The Secretary or other Agency official designated by the Secretary will keep the Senior Agency Official for Privacy and the Chief Information Officer informed on the status of any investigation or recovery efforts.

13. Individuals who routinely access PII and their supervisors must sign a document annually describing their responsibilities and the consequences for failure to protect PII.

14. Departmental Elements and their sites should maintain a log which tracks all activities—including dates and times of events, decisions and corrective actions—for incidents involving breaches of PII.

15. The Departmental Element program responsible for the breach of PII shall incur and be responsible for all costs associated with remediation including notification of affected or potentially-affected individuals.

CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 206.1, *DEPARTMENT OF ENERGY PRIVACY PROGRAM*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) site/facility management contractors whose contracts involve the design, development or operation of a Privacy Act System of Record. In addition, the Personally Identifiable Information (PII) requirements in this CRD apply to any site management contractor that handles PII.

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's or subcontractor's compliance with the requirements.

1. GENERAL REQUIREMENTS.

   a. Ensure compliance with privacy requirements, specifically those provided in the Privacy Act of 1974, as amended at Title 5 United States Code (U.S.C.) 552a, and take appropriate actions to assist DOE in complying with Section 208 of the E-Government Act of 2002, and Office of Management and Budget (OMB) directives.

   b. Ensure that contractor employees are aware of their responsibility for—

      (1) safeguarding Personally Identifiable Information (PII) and

      (2) complying with the Privacy Act.

2. SPECIFIC REQUIREMENTS. The contractor must do the following:

   a. Ensure contractor employees are made aware of their roles and responsibilities for reporting suspected or confirmed incidents involving the breach of PII.

   b. Ensure contractor employees are cognizant of the following DOE Privacy Rules of Conduct. At a minimum, ensure contractor employees—

      (1) are trained in their responsibilities regarding the safeguarding of PII;

      (2) do not disclose any PII contained in any SOR except as authorized;

      (3) report any known or suspected loss of control or unauthorized disclosure of PII;

      (4) observe the requirements of DOE directives concerning marking and safeguarding sensitive information, including, when applicable, DOE O 471.3, *Protecting and Identifying Official Use Only Information*;

(5) collect only the minimum PII necessary for the proper performance of a documented agency function;

(6) do not place PII on shared drives, intranets or websites without permission of the System Owner; and

(7) challenge anyone who asks to see the PII for which they are responsible.

c. Ensure that contractor employees complete the Annual Privacy Training and sign the completion certificate acknowledging their responsibility for maintaining and protecting Privacy Act information prior to being authorized access to all information systems.

d. Ensure contractor employees are cognizant of the fact that all personal information collected, maintained, used, or disseminated on behalf of the Agency must be maintained in a Privacy Act SOR.

e. Ensure that contractor employees recognize differences between PII and the Privacy Act and the different obligations created by both authorities. Most personal information about an individual will fall under both the Privacy Act and OMB directives governing the safeguarding of PII. However, contractors must be cognizant that these are two separate authorities that impose different responsibilities on federal and contractor employees for safeguarding information. PII that is in a SOR is subject to the restrictions and penalties of the Privacy Act.

f. Ensure contractor employees are cognizant of the fact that non-compliance with the Privacy Act carries criminal and civil penalties.

U.S. Department of Justice
Information regarding Identity Theft and Identity Fraud

What Are Identity Theft and Identity Fraud?

"But he that filches from me my good name/Robs me of that which not enriches him/And makes me poor indeed." - Shakespeare, Othello, act iii. Sc. 3.

The short answer is that identity theft is a crime. Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. These Web pages are intended to explain why you need to take precautions to protect yourself from identity theft. Unlike your fingerprints, which are unique to you and cannot be given to someone else for their use, your personal data especially your Social Security number, your bank account or credit card number, your telephone calling card number, and other valuable identifying data can be used, if they fall into the wrong hands, to personally profit at your expense. In the United States and Canada, for example, many people have reported that unauthorized persons have taken funds out of their bank or financial accounts, or, in the worst cases, taken over their identities altogether, running up vast debts and committing crimes while using the victims's names. In many cases, a victim's losses may include not only out-of-pocket financial losses, but substantial additional financial costs associated with trying to restore his reputation in the community and correcting erroneous information for which the criminal is responsible.

In one notorious case of identity theft, the criminal, a convicted felon, not only incurred more than $100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and handguns in the victim's name, but called his victim to taunt him -- saying that he could continue to pose as the victim for as long as he wanted because identity theft was not a federal crime at that time -- before filing for bankruptcy, also in the victim's name. While the victim and his wife spent more than four years and more than $15,000 of their own money to restore their credit and reputation, the criminal served a brief sentence for making a false statement to procure a firearm, but made no restitution to his victim for any of the harm he had caused. This case, and others like it, prompted Congress in 1998 to create a new federal offense of identity theft.

What Are The Most Common Ways To Commit Identity Theft Or Fraud?

Many people do not realize how easily criminals can obtain our personal data without having to break into our homes. In public places, for example, criminals may engage in "shoulder surfing" watching you from a nearby location as you punch in your telephone calling card number or credit card number or listen in on your conversation if you give your credit-card number over the telephone to a hotel or rental car company.

Even the area near your home or office may not be secure. Some criminals engage in "dumpster diving" going through your garbage cans or a communal dumpster or trash bin -- to obtain copies of your checks, credit card or bank statements, or other records that typically bear your name, address, and even your telephone number. These types of records make it easier for criminals to get control over accounts in your name and assume your identity.

If you receive applications for "preapproved" credit cards in the mail, but discard them without tearing up the enclosed materials, criminals may retrieve them and try to activate the cards for their use without your knowledge. (Some credit card companies, when sending credit cards, have adopted security measures that allow a card recipient to activate the card only from his or her home telephone number but this is not yet a universal practice.) Also, if your mail is delivered to a place where others have ready access to it, criminals may simply intercept and redirect your mail to another location.

In recent years, the Internet has become an appealing place for criminals to obtain identifying data, such as passwords or even banking information. In their haste to explore the exciting features of the Internet, many people respond to "spam" unsolicited E-mail that promises them some benefit but requests identifying data, without realizing that in many cases, the requester has no intention of keeping his promise. In some cases, criminals reportedly have used computer technology to obtain large amounts of personal data.

With enough identifying information about an individual, a criminal can take over that individual's identity to conduct a wide range of crimes: for example, false applications for loans and credit cards, fraudulent withdrawals from bank accounts, fraudulent use of telephone calling cards, or obtaining other goods or privileges which the criminal might be denied if he were to use his real name. If the criminal takes steps to ensure that bills for the falsely obtained credit cards, or bank statements showing the unauthorized withdrawals, are sent to an address other than the victim's, the victim may not become aware of what is happing until the criminal has already inflicted substantial damage on the victim's assets, credit, and reputation.

What's The Department Of Justice Doing About Identity Theft And Fraud?

The Department of Justice prosecutes cases of identity theft and fraud under a variety of federal statutes. In the fall of 1998, for example, Congress passed the Identity Theft and Assumption Deterrence Act . This legislation created a new offense of identity theft, which prohibits knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

18 U.S.C. § 1028(a)(7). This offense, in most circumstances, carries a maximum term of 15 years' imprisonment, a fine, and criminal forfeiture of any personal property used or intended to be used to commit the offense.

Schemes to commit identity theft or fraud may also involve violations of other statutes such as identification fraud (18 U.S.C. § 1028), credit card fraud (18 U.S.C. § 1029), computer fraud (18 U.S.C. § 1030), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), or financial institution fraud (18 U.S.C. § 1344). Each of these federal offenses are felonies that carry substantial penalties in some cases, as high as 30 years' imprisonment, fines, and criminal forfeiture.

Federal prosecutors work with federal investigative agencies such as the Federal Bureau of Investigation, the United States Secret Service, and the United States Postal Inspection Service to prosecute identity theft and fraud cases.

Here are some examples of recent cases:

Central District of California. A woman pleaded guilty to federal charges of using a stolen Social Security number to obtain thousands of dollars in credit and then filing for bankruptcy in the name of her victim. More recently, a man was indicted, pleaded guilty to federal charges and was sentenced to 27 months' imprisonment for obtaining private bank account information about an insurance company's policyholders and using that information to deposit $764,000 in counterfeit checks into a bank account he established.

Central District of California. Two of three defendants have pleaded guilty to identity theft, bank fraud, and related charges for their roles in a scheme to open bank accounts with both real and fake identification documents, deposit U.S. Treasury checks that were stolen from the mail, and withdraw funds from those accounts.

Middle District of Florida. A defendant has been indicted on bank fraud charges for obtaining names, addresses, and Social Security numbers from a Web site and using those data to apply for a series of car loans over the Internet.

Southern District of Florida. A woman was indicted and pleaded guilty to federal charges involving her obtaining a fraudulent driver's license in the name of the victim, using the license to withdraw more than $13,000 from the victim's bank account, and obtaining five department store credit cards in the victim's name and charging approximately $4,000 on those cards.

District of Kansas. A defendant pleaded guilty to conspiracy, odometer fraud, and mail fraud for operating an odometer "rollback" scheme on used cars. The defendant used false and assumed identities, including the identities of deceased persons, to obtain false identification documents and fraudulent car titles.

What Can I Do About Identity Theft And Fraud?

To victims of identity theft and fraud, the task of correcting incorrect information about their financial or personal status, and trying to restore their good names and reputations, may seem as daunting as trying to solve a puzzle in which some of the pieces are missing and other pieces no longer fit as they once did. Unfortunately, the damage that criminals do in stealing another person's identity and using it to commit fraud often takes far longer to undo than it took the criminal to commit the crimes.

What Should I Do To Avoid Becoming A Victim Of Identity Theft?

To reduce or minimize the risk of becoming a victim of identity theft or fraud, there are some basic steps you can take. For starters, just remember the word "**SCAM**":

S Be **stingy** about giving out your personal information to others unless you have a reason to trust them, regardless of where you are:

At Home.

1. Start by adopting a "need to know" approach to your personal data. Your credit card company may need to know your mother's maiden name, so that it can verify your identity when you call to inquire about your account. A person who calls you and says he's from your bank, however, doesn't need to know that information if it's already on file with your bank; the only purpose of such a call is to acquire that information for that person's personal benefit. Also, the more information that you have printed on your personal bank checks -- such as your Social Security number or home telephone number -- the more personal data you are routinely handing out to people who may not need that information.
2. If someone you don't know calls you on the telephone and offers you the chance to receive a "major" credit card, a prize, or other valuable item, but asks you for personal data -- such as your Social Security number, credit card number or expiration date, or mother's maiden name -- ask them to send you a written application form.
3. If they won't do it, tell them you're not interested and hang up.

4. If they will, review the application carefully when you receive it and make sure it's going to a company or financial institution that's well-known and reputable. The Better Business Bureau can give you information about businesses that have been the subject of complaints.

On Travel.

1. If you're traveling, have your mail held at your local post office, or ask someone you know well and trust another family member, a friend, or a neighbor to collect and hold your mail while you're away.
2. If you have to telephone someone while you're traveling, and need to pass on personal financial information to the person you're calling, don't do it at an open telephone booth where passersby can listen in on what you're saying; use a telephone booth where you can close the door, or wait until you're at a less public location to call.

C Check your financial information regularly, and look for what should be there and what shouldn't:

What Should Be There.

1. If you have bank or credit card accounts, you should be receiving monthly statements that list transactions for the most recent month or reporting period.
2. If you're not receiving monthly statements for the accounts you know you have, call the financial institution or credit card company immediately and ask about it.
3. If you're told that your statements are being mailed to another address that you haven't authorized, tell the financial institution or credit card representative immediately that you did not authorize the change of address and that someone may be improperly using your accounts. In that situation, you should also ask for copies of all statements and debit or charge transactions that have occurred since the last statement you received. Obtaining those copies will help you to work with the financial institution or credit card company in determining whether some or all of those debit or charge transactions were fraudulent.<

What Shouldn't Be There.

1. If someone has gotten your financial data and made unauthorized debits or charges against your financial accounts, checking your monthly statements carefully may be the quickest way for you to find out. Too many of us give those statements, or the enclosed checks or credit transactions, only a quick glance, and don't review them closely to make sure there are no unauthorized withdrawals or charges.
2. If someone has managed to get access to your mail or other personal data, and opened any credit cards in your name or taken any funds from your bank account, contact your financial institution or credit card company immediately to report those transactions and to request further action.

A Ask periodically for a copy of your credit report.

Your credit report should list all bank and financial accounts under your name, and will provide other indications of whether someone has wrongfully opened or used any accounts in your name.

M Maintain careful records of your banking and financial accounts.

Even though financial institutions are required to maintain copies of your checks, debit transactions, and similar transactions for five years, you should retain your monthly statements and checks for at least one year, if not more. If you need to dispute a particular check or transaction especially if they purport to bear your signatures your original records will be more immediately accessible and useful to the institutions that you have contacted.

Even if you take all of these steps, however, it's still possible that you can become a victim of identity theft. Records containing your personal data -- credit-card receipts or car-rental agreements, for example -- may be found by or shared with someone who decides to use your data for fraudulent purposes.

What Should I Do If I've Become A Victim Of Identity Theft?

If you think you've become a victim of identity theft or fraud, act immediately to minimize the damage to your personal funds and financial accounts, as well as your reputation. Here's a list -- based in part on a checklist prepared by the California Public Interest Research Group (CalPIRG) and the Privacy Rights Clearinghouse -- of some actions that you should take right away:

1. Contact the Federal Trade Commission (FTC) to report the situation, whether Online,
2. By telephone toll-free at 1-877-ID THEFT (877-438-4338) or TDD at 202-326-2502, or
3. By mail to Consumer Response Center, FTC, 600 Pennsylvania Avenue, N.W., Washington, DC 20580.

Under the Identity Theft and Assumption Deterrence Act , the Federal Trade Commission is responsible for receiving and processing complaints from people who believe they may be victims of identity theft, providing informational materials to those people, and referring those complaints to appropriate entities, including the major credit reporting agencies and law enforcement agencies. For further information, please check the FTC's identity theft Web pages . You can also call your local office of the FBI or the U.S. Secret Service to report crimes relating to identity theft and fraud.

You may also need to contact other agencies for other types of identity theft:

1. Your local office of the Postal Inspection Service if you suspect that an identity thief has submitted a change-of-address form with the Post Office to redirect your mail, or has used the mail to commit frauds involving your identity;
2. The Social Security Administration if you suspect that your Social Security number is being fraudulently used (call 800-269-0271 to report the fraud);
3. The Internal Revenue Service if you suspect the improper use of identification information in connection with tax violations (call 1-800-829-0433 to report the violations).

Call the fraud units of the three principal credit reporting companies:

Equifax:

1. To report fraud, call (800) 525-6285 or write to P.O. Box 740250, Atlanta, GA 30374-0250.
2. To order a copy of your credit report ($8 in most states), write to P.O. Box 740241, Atlanta, GA 30374-0241, or call (800) 685-1111.
3. To dispute information in your report, call the phone number provided on your credit report.

4. To opt out of pre-approved offers of credit, call (888) 567-8688 or write to Equifax Options, P.O. Box 740123, Atlanta GA 30374-0123.

Experian (formerly TRW)

1. To report fraud, call (888) EXPERIAN or (888) 397-3742, fax to (800) 301-7196, or write to P.O. Box 1017, Allen, TX 75013.
2. To order a copy of your credit report ($8 in most states): P.O. Box 2104, Allen TX 75013, or call (888) EXPERIAN.
3. To dispute information in your report, call the phone number provided on your credit report.
4. To opt out of pre-approved offers of credit and marketing lists, call (800) 353-0809 or (888) 5OPTOUT or write to P.O. Box 919, Allen, TX 75013.

Trans Union

1. To report fraud, call (800) 680-7289 or write to P.O. Box 6790, Fullerton, CA 92634.
2. To order a copy of your credit report ($8 in most states), write to P.O. Box 390, Springfield, PA 19064 or call: (800) 888-4213.
3. To dispute information in your report, call the phone number provided on your credit report.
4. To opt out of pre-approved offers of credit and marketing lists, call (800) 680-7293 or (888) 5OPTOUT or write to P.O Box 97328, Jackson, MS 39238.

Contact all creditors with whom your name or identifying data have been fraudulently used. For example, you may need to contact your long-distance telephone company if your long-distance calling card has been stolen or you find fraudulent charges on your bill.

Contact all financial institutions where you have accounts that an identity thief has taken over or that have been created in your name but without your knowledge. You may need to cancel those accounts, place stop-payment orders on any outstanding checks that may not have cleared, and change your Automated Teller Machine (ATM) card, account, and Personal Identification Number (PIN).

Contact the major check verification companies (listed in the CalPIRG-Privacy Rights Clearinghouse checklist) if you have had checks stolen or bank accounts set up by an identity thief. In particular, if you know that a particular merchant has received a check stolen from you, contact the verification company that the merchant uses:

1. CheckRite -- (800) 766-2748
2. ChexSystems -- (800) 428-9623 (closed checking accounts)
3. CrossCheck -- (800) 552-1900
4. Equifax -- (800) 437-5120
5. National Processing Co. (NPC) -- (800) 526-5380
6. SCAN -- (800) 262-7771
7. TeleCheck -- (800) 710-9898

U.S. Department of Justice
Information on Internet Fraud

What Is Internet Fraud?

The term "Internet fraud" refers generally to any type of fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme.

If you use the Internet with any frequency, you'll soon see that people and things online tend to move, as the saying goes, on "Internet time." For most people, that phrase simply means that things seem to happen more quickly on the Internet -- business decisions, information-searching, personal interactions, to name a few - and to happen before, during, or after ordinary "bricks-and-mortar" business hours.

Unfortunately, people who engage in fraud often operate in "Internet time" as well. They seek to take advantage of the Internet's unique capabilities -- for example, by sending e-mail messages worldwide in seconds, or posting Web site information that is readily accessible from anywhere in the world - to carry out various types of fraudulent schemes more quickly than was possible with many fraud schemes in the past.

What Are The Major Types of Internet Fraud?

In general, the same types of fraud schemes that have victimized consumers and investors for many years before the creation of the Internet are now appearing online (sometimes with particular refinements that are unique to Internet technology). With the explosive growth of the Internet, and e-commerce in particular, online criminals try to present fraudulent schemes in ways that look, as much as possible, like the goods and services that the vast majority of legitimate e-commerce merchants offer. In the process, they not only cause harm to consumers and investors, but also undermine consumer confidence in legitimate e-commerce and the Internet.

Here are some of the major types of Internet fraud that law enforcement and regulatory authorities and consumer organizations are seeing:

Auction and Retail Schemes Online. According to the Federal Trade Commission and Internet Fraud Watch, fraudulent schemes appearing on online auction sites are the most frequently reported form of Internet fraud. These schemes, and similar schemes for online retail goods, typically purport to offer high-value items - ranging from Cartier® watches to computers to collectibles such as Beanie Babies® - that are likely to attract many consumers. These schemes induce their victims to send money for the promised items, but then deliver nothing or only an item far less valuable than what was promised (e.g., counterfeit or altered goods).

Business Opportunity/"Work-at-Home" Schemes Online. Fraudulent schemes often use the Internet to advertise purported business opportunities that will allow individuals to earn thousands of dollars a month in "work-at-home" ventures. These schemes typically require the individuals to pay anywhere from $35 to several hundred dollars or more, but fail to deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business.

Identity Theft and Fraud. Some Internet fraud schemes also involve identity theft - the wrongful obtaining and using of someone else's personal data in some way that involves fraud or deception, typically for economic gain.

In one federal prosecution, the defendants allegedly obtained the names and Social Security numbers of U.S. military officers from a Web site, then used more than 100 of those names and numbers to apply via the Internet for credit cards with a Delaware bank.

In another federal prosecution, the defendant allegedly obtained personal data from a federal agency's Web site, then used the personal data to submit 14 car loan applications online to a Florida bank.

Investment Schemes Online

Market Manipulation Schemes. Enforcement actions by the Securities and Exchange Commission and criminal prosecutions indicate that criminals are using two basic methods for trying to manipulate securities markets for their personal profit. First, in so-called "pump-and-dump" schemes, they typically disseminate false and fraudulent information in an effort to cause dramatic price increases in thinly traded stocks or stocks of shell companies (the "pump"), then immediately sell off their holdings of those stocks (the "dump") to realize substantial profits before the stock price falls back to its usual low level. Any other buyers of the stock who are unaware of the falsity of the information become victims of the scheme once the price falls.
For example, in one federal prosecution in Los Angeles, the defendants allegedly purchased, directly and through another man, a total of 130,000 shares in a bankrupt company, NEI Webworld, Inc., whose assets had been liquidated several months earlier. The defendants then allegedly posted bogus e-mail messages on hundreds of Internet bulletin boards, falsely stating that NEI Webworld was going to be taken over by a wireless telecommunications company. At the time of the defendants' alleged purchases of NEI Webworld stock, the stock was priced between 9 cents and 13 cents a share. Ultimately, in a single morning of trading, NEI Webworld stock rose in 45 minutes from $8 per share to a high of $15 5/16, before falling, within a half-hour, to 25 cents per share. The defendants allegedly realized profits of $362,625.

In another federal prosecution in Los Angeles, a man who worked for a California company, PairGain Technologies, created a bogus Bloomberg news Web site which falsely reported that PairGain was about to be acquired by an Israeli company, and posted fraudulent e-mail messages, containing links to the counterfeit Bloomberg news site, on financial news bulletin boards. On the day that the bogus report was posted on the Internet, PairGain stock rose approximately 30 percent before PairGain issued its own press release stating that the report was false.

Second, in short-selling or "scalping" schemes, the scheme takes a similar approach, by disseminating false or fraudulent information in an effort to cause price decreases in a particular company's stock.

For example, in one recent federal prosecution, a man who described himself as a "day trader" allegedly posted (more than 20 times) a bogus press release falsely stating that a major telecommunications- and Internet-related company, Lucent Technologies, Inc., would not meet its quarterly earnings estimates. The day trader allegedly traded approximately 6,000 shares of Lucent stock the same day that he posted the bogus press release. The false reports allegedly drove the stock's price down 3.6 percent and reduced Lucent's market value by more than $7 billion.

Other Investment Schemes Other types of fraudulent investment schemes may combine uses of the Internet with traditional mass-marketing technology such as telemarketing to reach large numbers of potential victims.

In a federal prosecution in San Diego, a major fraudulent scheme used the Internet and telemarketing to solicit prospective investors for so-called "general partnerships" involving purported "high-tech" investments, such as an Internet shopping mall and Internet access providers. The scheme allegedly defrauded more than 3,000 victims nationwide of nearly $50 million.

Credit-Card Schemes. Some Internet fraud schemes, which appear to be variations on the online auction schemes described earlier, involve the use of unlawfully obtained credit card numbers to order goods or services online.

One widely reported and intricate scheme, for example, involves offering consumers high-value consumer items, such as video cameras, at a very attractive price (i.e., below the price set at legitimate e-commerce Web sites). When a potential consumer contacts the "seller," the "seller" promises to ship the consumer the item before the consumer has to pay anything. If the consumer agrees, the "seller" (without the consumer's knowledge) uses that consumer's real name, along with an unlawfully obtained credit card number belonging to another person, to buy the item at a legitimate Web site. Once that Web site ships the item to the consumer, the consumer, believing that the transaction is legitimate, then authorizes his credit card to be billed in favor of the "seller" or sends payment directly to the "seller."

As a result, there are two victims of the scheme: the original e-commerce merchant who shipped the item based on the unlawfully used credit card; and the consumer who sent his money after receiving the item that the "seller" fraudulently ordered from the merchant. In the meantime, the "seller" may have transferred his fraudulent proceeds to bank accounts beyond the effective reach of either the merchant or the consumer.

Other Schemes. Some Web sites on the Internet have purported to offer those who want a "quick divorce" an opportunity to obtain a divorce in the Dominican Republic or other foreign countries for $1,000 or more, without even having to leave the United States. These sites often contain false, misleading, or legally inaccurate information about the process for obtaining such divorces (e.g., that neither spouse has to visit the country in which the divorce is being sought). Typically, people who have sent money to one of these schemes eventually receive false assurances that they are legally divorced. In fact, victims of the scheme have neither received legitimate legal services nor obtained valid divorces. People who are interested in obtaining a divorce, whether in the United States or elsewhere, should seek a lawyer with whom they can speak personally, and not rely solely on e-mail exchanges or online information.

What Is The Department of Justice Doing About Internet Fraud?

Since February 1999, when the Department of Justice established its Internet Fraud Initiative, the federal government has been expanding its efforts to combine criminal prosecution with coordinated analysis and investigation as part of a comprehensive approach to combating Internet fraud.

Prosecution

The Justice Department has begun to bring a number of criminal prosecutions throughout the country against individuals and groups engaging in various types of Internet fraud. Here are some examples of federal criminal prosecutions directed at Internet fraud:

Auction and Retail Schemes Online

Oxford, Mississippi On August 27, 1998, a woman was sentenced in the Northern District of Mississippi to 15 months' imprisonment and $9,432 restitution on fraud charges relating to her conduct of a fraudulent scheme. The scheme involved her use of Web pages and interactive computer locations on the Internet for falsely advertising various computer hardware and software and computer accessories.

Philadelphia On March 2, 2000, three men were criminally charged in the Eastern District of Pennsylvania for their alleged roles in falsely offering the sale of Beanie Babies® on the Internet, and then failing to deliver the orders or sending stolen Beanie Babies® that generally were of substantially less value than the items ordered.

San Diego On March 6, 2000, a man pleaded guilty in the Southern District of California to mail and wire fraud in connection with his conduct of a fraudulent scheme involving Internet sales of Beanie Babies® that he never delivered.

Santa Ana, California On November 1, 1999, a man was sentenced in the Central District of California on mail and credit-card fraud charges to 14 months' imprisonment and $36,000 restitution, for his conduct of an Internet auction fraud that falsely offered digital cameras and laptop computers to consumers.

Seattle On August 6, 1999, a man pleaded guilty in the Western District of Washington to wire fraud in connection with his role in placing on various Web sites false advertisements for computer systems, for which he accepted victims' payments but which he never delivered.

West Palm Beach, Florida On February 12, 1999, a man was sentenced in the Southern District of Florida on wire fraud charges to six months home detention and more than $22,000 restitution, for his conduct of a fraudulent scheme in which he falsely advertised on Internet auction and retail sale Web sites computer components that he purported to have for sale, but did not have or obtain most of the merchandise he advertised.

Business-Opportunity Schemes Online

Los Angeles In November, 1999, four individuals were criminally charged in the Central District of California for their roles in conducting a fraudulent scheme, in which they sent out approximately 50 million e-mails that falsely advertised work-at-home opportunities for people but provided few actual opportunities for people who paid the $35 advance fee.

Investment Schemes Online "Pump-and-dump" schemes, short-selling schemes, Ponzi schemes, and other fraudulent investment schemes have all been subjects of federal prosecution throughout the country.

Alexandria, Virginia In September 1997, a man was sentenced in the Eastern District of Virginia to one year's imprisonment and fined $20,000 on securities fraud conspiracy charges relating to his touting of a stock involved in a "pump and dump" scheme.

Brooklyn, New York In August, 1999, four individuals were indicted in the Eastern District of New York on securities fraud charges for their alleged roles in the fraudulent promotion of eight stocks through misleading Internet Web site and e-mail newsletter profiles.

Charlotte, North Carolina In 1999, two individuals pleaded guilty in the Western District of North Carolina to securities fraud charges for their roles in offering securities in a nonexistent investment bank that purportedly offered, among other things, a "guaranteed" 20 percent return on savings.

Cleveland On March 22, 2000, four people were indicted in the Northern District of Ohio, on charges including conspiracy to commit and committing mail and wire fraud. The defendants allegedly devised and carried out a scheme to defraud "investors" in a "Ponzi" pyramid scheme. A company with which the defendants were affiliated allegedly collected more than $26 million from "investors" without selling any product or service, and paid older investors with the proceeds of the money collected from the newer investors.

Los Angeles On January 4, 2000, two men were indicted in the Central District of California on securities fraud charges for their alleged roles in the NEI Webworld scheme described earlier. In addition, on August 30, 1999, the individual who conducted the PairGain Technologies scheme mentioned earlier was sentenced in the Central District of California to five months' home detention and $93,000 restitution.

New York On August 9, 1999, a man was criminally charged in the Southern District of New York with securities fraud. The man allegedly conducted a scheme to unlawfully inflate the price of stock of a company involved in acquiring retail auto dealerships, by making various false claims that another company (located in the same office suite as the auto dealership company) had developed a cure for HIV infection and AIDS.

Credit Card Fraud

Ft. Lauderdale In November, 1997, a former graduate student was sentenced in the Southern District of Florida on wire fraud charges to four months' home detention, for a scheme in which he obtained the names of multiple students from a local university and fraudulently applied for 174 credit cards via the Internet. Because of the quick investigative work by the Postal Inspection Service, no losses were incurred.

Wilmington, Delaware In 2000, three individuals were indicted in the District of Delaware on charges of conspiracy, bank fraud, identity theft, Social Security fraud, and wire fraud, for their alleged roles in the military officers' Social Security number/credit-card fraud scheme described earlier.

Other Types of Internet Fraud

Los Angeles On February 7, 2000, a man was sentenced to 87 months' imprisonment for his role in a scheme that purported to provide immigration assistance to aliens seeking to become residents or citizens of the United States. Using Web sites, newspaper advertisements, recruiters, and word of mouth to offer their services to aliens, the leaders of the scheme typically charged more than $10,000 per client and promised that the client would receive particular immigration documents. In some cases, however, the leaders of the scheme provided their clients with counterfeit or false immigration documents; in other cases, they provided no documents at all, and blamed the government and the legal system for the delay in providing the promised documents.

Los Angeles In November, 1999, four men were criminally charged in the Central District of California for their alleged roles in conducting the "work-at-home" scheme described earlier.
-top-

National Coordination and Cooperation

The global nature of the Internet, and law enforcement experience in conducting Internet fraud investigations, have made it increasingly clear that law enforcement authorities need to work in closer coordination to have a substantial effect on all forms of Internet fraud. Two major steps that the Department has taken to foster national coordination and cooperation among law enforcement authorities on Internet fraud matters are the Internet Fraud Initiative and the Internet Fraud Complaint Center.

The Internet Fraud Initiative, which the Attorney General approved on February 26, 1999, is a national initiative by the Department of Justice intended to provide a comprehensive approach to combating Internet fraud. The Initiative has six main elements:

(1) Developing information on the nature and scope of the problem, through coordination with the Federal Trade Commission on Internet fraud data, and exploring the development of methods for reliable estimates of the prevalence and incidence of Internet fraud;

(2) Developing and providing specific joint training for prosecutors and agents on Internet fraud, through National Advocacy Center (NAC) training at basic and advanced levels, other federal law enforcement training programs, and coordination with joint training efforts by the National Association of Attorneys General and the American Prosecutors Research Institute for state and local law enforcement;

(3) Fostering the development of investigative and analytical resources to identify and investigate Internet-related fraud schemes, by supporting joint FBI-National White Collar Crime Center efforts to establish the Internet Fraud Complaint Center and forging closer ties and establishing referral procedures with other federal agencies;

(4) Providing and facilitating coordination among federal prosecutors, the Department and other federal law enforcement and regulatory agencies, and state, local, and foreign law enforcement agencies on Internet fraud investigations and prosecutions;

(5) Supporting and advising on Internet fraud prosecutions throughout the country; and

(6) Establishing a program of public education and prevention on Internet fraud, including encouraging the private sector to use technological solutions (such as biometrics) to prevent frauds, adding Internet fraud pages to the Department's Web site, and expanding public-private prevention efforts;

The Internet Crime Complaint Center (IC3) is a joint project of the FBI and the National White Collar Crime Center. The IC3's key functions for federal, state, and local law enforcement agencies will be (1) receiving online complaints, (2) analyzing them to identify particular schemes and general crime trends in Internet fraud, and (3) compiling and referring potential Internet fraud schemes to law enforcement. In addition to FBI and NWCCC personnel, the IFCC will include agents and analysts detailed from the Internal Revenue Service and Postal Inspection Service.

In effect, the IC3 provides federal, state, and local law enforcement agencies with a single point of contact - a "one-stop-shopping" approach - for identifying and referring Internet fraud schemes for criminal enforcement. Because criminal fraud schemes on the Internet, such as major investment or credit card frauds, can be initiated and concluded in a matter of days or even hours, traditional methods of investigating fraud schemes will no longer suffice. By co-locating agents and analysts from the FBI, the NWCCC, and other agencies, the IC3 can provide a substantial investigative and analytical resource available on a nationwide basis to law enforcement and regulatory agencies.

How Should I Deal With Internet Fraud?

Judging by the sheer number of solicitations and "can't miss" propositions that you can see every day in your e-mail mailbox or posted on message boards or Web sites, Internet scams may seem inescapable. While you can't wholly avoid seeing online solicitations that may be fraudulent, here are some tips on how to deal with them.

GENERAL TIPS ON POSSIBLE INTERNET FRAUD SCHEMES

Don't Judge by Initial Appearances. It may seem obvious, but consumers need to remember that just because something appears on the Internet - no matter how impressive or professional the Web site looks - doesn't mean it's true. The ready availability of software that allows anyone, at minimal cost, to set up a professional-looking Web site means that criminals can make their Web sites look as impressive as those of legitimate e-commerce merchants.

Be Careful About Giving Out Valuable Personal Data Online. If you see e-mail messages from someone you don't know that ask you for personal data - such as your Social Security number, credit-card number, or password - don't just send the data without knowing more about who's asking. Criminals have been known to send messages in which they pretend to be (for example) a systems administrator or Internet service provider representative in order to persuade people online that they should disclose valuable personal data. While secure transactions with known e-commerce sites are fairly safe, especially if you use a credit card, nonsecure messages to unknown recipients are not.

Be Especially Careful About Online Communications With Someone Who Conceals His True Identity. If someone sends you an e-mail in which he refuses to disclose his full identity, or uses an e-mail header that has no useful identifying data (e.g., "W6T7S8@provider.com"), that may be an indication that the person doesn't want to leave any information that could allow you to contact them later if you have a dispute over undelivered goods for which you paid. As a result, you should be highly wary about relying on advice that such people give you if they are trying to persuade you to entrust your money to them.

Watch Out for "Advance-Fee" Demands. In general, you need to look carefully at any online seller of goods or services who wants you to send checks or money orders immediately to a post office box, before you receive the goods or services you've been promised. Legitimate startup "dot.com" companies, of course, may not have the brand-name recognition of long-established companies, and still be fully capable of delivering what you need at a fair price. Even so, using the Internet to research online companies that aren't known to you is a reasonable step to take before you decide to entrust a significant amount of money to such companies.

TIPS ON SPECIFIC INTERNET FRAUD SCHEMES
- AUCTION AND RETAIL SALES SCHEMES

To reduce the chances that you may be victimized by fraudulent online auction or retail sales schemes, here are two basic tips:

Research The Prospective Seller Carefully. If you haven't had personal (and favorable) experience with someone who's offering certain goods for online sale or auction, look for sources of information at the Web site where the offeror's information is posted, and at other Web sites. Some online auction sites provide their member with opportunities to provide "feedback" on their experiences with particular sellers (although certain sellers have tried to manipulate the "feedback" process by posting favorable but false reports about themselves).

Pay by Credit Card or Escrow Service If Possible. If you charge your online purchase on a major U.S. bank-issued credit card, your liability may be limited to $50 under any circumstances, and at least one credit-card issuer has recently indicated that it will waive the $50 deductible. In the alternative, some online auction Web sites offer escrow services that (for a small percentage) will guarantee delivery of the ordered goods before releasing your payment to the seller.
-top-

- INVESTMENT SCHEMES ONLINE
To reduce your risks from online investment opportunities that may be fraudulent, here are four basic tips:

Take Your Time In Making Investment Decisions. Remember that in any "get-rich-quick" scheme, there's only one person who's guaranteed to get rich quick: the person promoting the scheme.
If you're thinking about pursuing some online investment opportunity, start by recognizing that you need to take your time in making decisions about what you do with your hard-earned money. Sound investing for the long term takes patience, the will to ignore momentary market fluctuations, and a carefully thought-out plan for reaching your investment goals.

Whether you're researching an investment opportunity on the Web, or talking with a broker or someone else who's offering you the opportunity, you should make it a habit to take notes of what you're reading or hearing. The North American Securities Administrators Association (NASAA) publishes an investor's notepad entitled, "When Your Broker Calls, Take Notes!" The forms are printed in notepad fashion so investors can get into the habit of making written records of their conversations with their brokers. The notepad is available from your state securities regulators or on the NASAA website at www.nasaa.org/whoweare/media/Notepad.html.
Research The Potential Investment Opportunity - And Who's Behind It - Carefully. If you're making a major investment decision, here's an easy rule of thumb: Count how many weeks, months, or years it took you to earn that amount of money, and then resolve to spend at least that many days to research the investment opportunity and the people who are promoting or running it.

Several agencies and self-regulatory organizations can give you a substantial hand with your research, at no cost to you:

The SEC's Web site, www.sec.gov, contains a wealth of information about many companies, in at least two principal sources: (1) reports these companies file electronically through the EDGAR system; and (2) the SEC Enforcement Division's online files, which among other things list the persons against whom the SEC has filed civil enforcement actions for securities law violations (and, in some cases, against whom the Department of Justice or state or local prosecutors have filed criminal charges). You can use the built-in search engine at the SEC's Web site to check out names, and see whether you get any hits in the SEC enforcement action listings. The site also contains some excellent lists of questions to ask about any investment opportunity, and a discussion of how to spot signs of online investment scams.

The Federal Trade Commission's Web site, www.ftc.gov, also has an internal search engine, which allows you to look for information on particular individuals or companies involved with your prospective investment, including listings of FTC enforcement actions.

The National Association of Securities Dealers (NASD) allows you to check for some disciplinary history on the broker or company that's touting a particular investment. Go to www.nasdr.com or call the NASD's Public Disclosure hotline at 800-289-9999.
State securities regulators in your state may also have information on the company or its organizers that you can obtain. Check your local telephone listings for the securities regulator in your state, or go to the North American Securities Administrators Association's Web site, www.nasaa.org, for a listing of state and provincial securities regulators in the United States, Canada, and Mexico.

If the potential investment involves commodities, you may also need to check out the Commodity Futures Trading Commission's Web site, www.cftc.gov, and use its internal search engine to check out companies and people. The National Futures Association can also give you information on the disciplinary history of brokers or other commodity professionals, the registration status of firms and individuals, and arbitration and mediation procedures. Call them at 1-800-676-4NFA between 8:00 a.m. and 5:00 p.m. Central Time or go to www.nfa.futures.org.

If the prospective investment supposedly involves an Internet financial institution, go to the Federal Deposit Insurance Corporation (FDIC)'s Online Banks Web pages, and use the FDIC's Financial Institutions Search Engine you find there to see whether the financial institution has a legitimate banking charter and is a member of the FDIC.

When the potential investment is based outside the United States, remember that your money may be even more at risk, as you may have little or no recourse in the event of loss. The United Kingdom's Financial Services Authority allows investors to check out U.K. and European Union-based investment offers at its Central Register (call 01-71-929-3652).

Finally, use one or more of the many Internet search engines - like the ones available on your Web browser - to help you expand your research on the company's background and market performance.
If you use these resources, and find that one or more of the people behind your prospective investment has been subject to legal action, especially for investment offers, it's a very safe bet that the investment is a high risk at best and an outright scam at worst.
-top-

Boilers and "Boiler Rooms" Need High Pressure To Do Their Jobs. If someone online is insisting that you invest right away, or telling you that someone else will get the "deal of a lifetime" if you wait, ask yourself at that moment whether you're feeling pressured and uncomfortable. If you are, that's a major red flag warning you away from the investment. Legitimate businesspeople and brokers don't need to subject you to "high-pressure" tactics to make you commit to an investment decision before you're ready. That's why the operations scam artists run are called "boiler rooms": like steam boilers, high pressure is what they're designed to generate (along with a wide array of lies, half-truths, and deceptive statements).

Even if you're in a chat room or online discussion group where everyone seems to be "just like you," enthusiastic about investing and looking for the next great investment, not everyone who's online at that moment is necessarily just like you. Some of the messages you see may be coming from someone working for the investment scheme's organizers - or even one of the organizers himself - who pretends to be someone else, so they can pressure you in less obvious ways and get you to fall for the scheme.

Check Out The Competition. If someone's promising you returns on investment that are far above what you see in the financial pages of your newspaper or at your local bank, ask yourself how they can possibly guarantee those fabulous returns.

Sometimes it's because, as in any good old-fashioned Ponzi scheme, they're paying older investors with money that newer investors gave them, and they're trying to string out the fraud to rope in as many investors as possible. Sometimes it's because they'll promise you anything, but give you nothing once you've entrusted your money to them.

If, after you've gone through all of the steps listed above, you still feel like the prospective investment is worth considering, talk to a broker, financial adviser, or banker with whom you've done business for a while, and ask whether his or her firm or financial institution can offer you a comparable type of investment with less risk.

The chances are that they'll say no, but they'll be willing to take time with you to walk through the information you have about the prospective investment and point out the risks you may be taking, as well as possible alternative investments that offer more realistic returns.

You lose nothing by consulting an investment professional about any major investment decision - and you stand to lose a lot if you don't.

FILING COMPLAINTS ABOUT INTERNET FRAUD

If you think that you've been the victim of a fraud scheme that involved the Internet, you can file a complaint online with the Internet Crime Complaint Center, a joint project of the FBI and the National White Collar Crime Center. In addition, you can file complaints about specific types of fraud complaints with the following agencies:

Commodities Fraud: Commodity Futures Trading Commission (CFTC)
Consumer Fraud: Federal Trade Commission

Securities Fraud: SEC Enforcement Division Complaint Center or your state securities regulators.

Home | Previous Page

U.S. Securities and Exchange Commission

Internet Fraud: How to Avoid Internet Investment Scams

The Internet serves as an excellent tool for investors, allowing them to easily and inexpensively research investment opportunities. But the Internet is also an excellent tool for fraudsters. That's why you should always think twice *before* you invest your money in any opportunity you learn about through the Internet.

This alert tells you how to spot different types of Internet fraud, what the SEC is doing to fight Internet investment scams, and how to use the Internet to invest wisely.

Navigating the Frontier: Where the Frauds Are

The Internet allows individuals or companies to communicate with a large audience without spending a lot of time, effort, or money. Anyone can reach tens of thousands of people by building an Internet web site, posting a message on an online bulletin board, entering a discussion in a live "chat" room, or sending mass e-mails. It's easy for fraudsters to make their messages look real and credible. But it's nearly impossible for investors to tell the difference between fact and fiction.

Online Investment Newsletters

Hundreds of online investment newsletters have appeared on the Internet in recent years. Many offer investors seemingly unbiased information free of charge about featured companies or recommending "stock picks of the month." While legitimate online newsletters can help investors gather valuable information, some online newsletters are tools for fraud.

Some companies pay the people who write online newsletters cash or securities to "tout" or recommend their stocks. While this isn't illegal, the federal securities laws require the newsletters to disclose who paid them, the amount, and the type of payment. But many fraudsters fail to do so. Instead, they'll lie about the payments they received, their independence, their so-called research, and their track records. Their newsletters masquerade as sources of unbiased information, when in fact they stand to profit handsomely if they convince investors to buy or sell particular stocks.

Some online newsletters falsely claim to independently research the stocks they profile. Others spread false information or promote worthless stocks. The most notorious sometimes "scalp" the stocks they hype, driving up the price of the stock with their baseless recommendations and then selling their own holdings at high prices and high profits. To learn how to separate the good from the bad, read our tips for checking out newsletters.

Bulletin Boards

Online bulletin boards – whether newsgroups, usenet, or web-based bulletin boards – have become an increasingly popular forum for investors to share information. Bulletin boards typically feature "threads" made up of numerous messages on various investment opportunities.

While some messages may be true, many turn out to be bogus – or even scams. Fraudsters often pump up a company or pretend to reveal "inside" information about upcoming announcements, new products, or lucrative contracts.

Also, you never know for certain who you're dealing with – or whether they're credible – because many bulletin boards allow users to hide their identity behind multiple aliases. People claiming to be unbiased observers who've carefully researched the company may actually be company insiders, large shareholders, or paid promoters. A single person can easily create the illusion of widespread interest in a small, thinly-traded stock by posting a series of messages under various aliases.

E-mail Spams

Because "spam" – junk e-mail – is so cheap and easy to create, fraudsters increasingly use it to find investors for bogus investment schemes or to spread false information about a company. Spam allows the unscrupulous to target many more potential investors than cold calling or mass mailing. Using a bulk e-mail program, spammers can send personalized messages to thousands and even millions of Internet users at a time.

How to Use the Internet to Invest Wisely

If you want to invest wisely and steer clear of frauds, you must get the facts. Never, ever, make an investment based solely on what you read in an online newsletter or bulletin board posting, especially if the investment involves a small, thinly-traded company that isn't well known. And don't even think about investing on your own in small companies that don't file regular reports with the SEC, unless you are willing to investigate each company thoroughly and to check the truth of every statement about the company. For instance, you'll need to:

- get financial statements from the company and be able to analyze them;

- verify the claims about new product developments or lucrative contracts;
- call every supplier or customer of the company and ask if they really do business with the company; and
- check out the people running the company and find out if they've ever made money for investors before.

And it doesn't stop there. For a more detailed list of questions you'll need to ask – and have answered – read *Ask Questions*. And always watch out for tell-tale signs of fraud.

Here's how you can use the internet to help you invest wisely:

Start With the SEC's EDGAR Database

The federal securities laws require many public companies to register with the SEC and file annual reports containing audited financial statements. For example, the following companies must file reports with the SEC:

- All U.S. companies with more than 500 investors *and* $10 million in net assets; and
- All companies that list their securities on The Nasdaq Stock Market or a major national stock exchange such as the New York Stock Exchange.

Anyone can access and download these reports from the SEC's EDGAR database for free. Before you invest in a company, check to see whether it's registered with the SEC and read its reports.

But some companies don't have to register their securities or file reports on EDGAR. For example, companies raising less than $5 million in a 12-month period may be exempt from registering the transaction under a rule known as "Regulation A." Instead, these companies must file a hard copy of the "offering circular" with the SEC containing financial statements and other information. Also, smaller companies raising less than one million dollars don't have to register with the SEC, but they must file a "Form D." Form D is a brief notice which includes the names and addresses of owners and stock promoters, but little other information. If you can't find a company on EDGAR, call the SEC at (202) 551-8090 to find out if the company filed an offering circular under Regulation A or a Form D. And be sure to request a copy.

The difference between investing in companies that register with the SEC and those that don't is like the difference between driving on a clear sunny day and driving at night without your headlights. You're asking for serious losses if you invest in small, thinly-traded companies that aren't widely known just by following the signs you read on Internet bulletin boards or online newsletters.

Contact Your State Securities Regulators

Don't stop with the SEC. You should always check with your state securities regulator, which you can find on the website of the North American Securities Administrators Association, to see if they have more information about the company and the people behind it. They can check the Central Registration Depository (CRD) and tell you whether the broker touting the stock or the broker's firm has a disciplinary history. They can also tell you whether they've cleared the offering for sale in your state.

Check with the Financial Industry Regulatory Authority (FINRA)

To check the disciplinary history of the broker or firm that's touting the stock, use FINRA's BrokerCheck website, or call FINRA's BrokerCheck Program hotline at (800) 289-9999.

Online Investment Fraud:
New Medium, Same Old Scam

The types of investment fraud seen online mirror the frauds perpetrated over the phone or through the mail. Remember that fraudsters can use a variety of Internet tools to spread false information, including bulletin boards, online newsletters, spam, or chat (including Internet Relay Chat or Web Page Chat). They can also build a glitzy, sophisticated web page. All of these tools cost very little money and can be found at the fingertips of fraudsters.

Consider all offers with skepticism. Investment frauds usually fit one of the following categories:

The "Pump And Dump" Scam

It's common to see messages posted online that urge readers to buy a stock quickly or tell you to sell before the price goes down. Often the writers will claim to have "inside" information about an impending development or to use an "infallible" combination of economic and stock market data to pick stocks. In reality, they may be insiders or paid promoters who stand to gain by selling their shares after the stock price is pumped up by gullible investors. Once these fraudsters sell their shares and stop hyping the stock, the price typically falls and investors lose their money. Fraudsters frequently use this ploy with small, thinly-traded companies because it's easier to manipulate a stock when there's little or no information available about the company.

The Pyramid

Be wary of messages that read: "How To Make Big Money From Your Home Computer!!!" One online promoter claimed that investors could "turn $5 into $60,000 in just three to six weeks." In reality, this program was nothing more than an electronic version of the classic "pyramid" scheme in which participants attempt to make money solely by recruiting new participants into the program.

The "Risk-Free" Fraud

"Exciting, Low-Risk Investment Opportunities" to participate in exotic-sounding investments – such as wireless cable projects, prime bank securities, and eel farms – have been offered through the Internet. But no investment is risk-free. And sometimes the investment products touted do not even exist – they're merely scams. Be wary of opportunities that promise spectacular profits or "guaranteed" returns. If the deal sounds too good to be true, then it probably is.

Off-shore Frauds

At one time, off-shore schemes targeting U.S. investors cost a great deal of money and were difficult to carry out. Conflicting time zones, differing currencies, and the high costs of international telephone calls and overnight mailings made it difficult for fraudsters to prey on U.S. residents. But the Internet has removed those obstacles. Be extra careful when considering any investment opportunity that comes from another country, because it's difficult for U.S. law enforcement agencies to investigate and prosecute foreign frauds.

The SEC Is Tracking Fraud

The SEC actively investigates allegations of Internet investment fraud and, in many cases, has taken quick action to stop scams. We've also coordinated with federal and state criminal authorities to put Internet fraudsters in jail. Here's a sampling of recent cases in which the SEC took action to fight Internet fraud:

Francis A. Tribble and Sloane Fitzgerald, Inc. sent more than six million unsolicited e-mails, built bogus web sites, and distributed an online newsletter over a ten-month period to promote two small, thinly traded "microcap" companies. Because they failed to tell investors that the companies they were touting had agreed to pay them in cash and securities, the SEC sued both Tribble and Sloane to stop them from violating the law again and imposed a $15,000 penalty on Tribble. Their massive spamming campaign triggered the largest number of complaints to the SEC's online Enforcement Complaint Center.

Charles O. Huttoe and twelve other defendants secretly distributed to friends and family nearly 42 million shares of Systems of Excellence Inc., known by its ticker symbol "SEXI." Huttoe drove up the price of SEXI shares through false press releases claiming non-existent multi-million dollar sales, an acquisition that had not occurred, and revenue projections that had no basis in reality. He also bribed co-defendant SGA Goldstar to tout SEXI to subscribers of SGA Goldstar's online "Whisper Stocks" newsletter. The SEC obtained court orders freezing Huttoe's assets and those of various others who participated in the scheme or who received fraud proceeds. Six people, including Huttoe and Theodore R. Melcher, Jr., the author of the online newsletter, were also convicted of criminal violations. Both Huttoe and Melcher were sentenced to federal prison. The SEC has thus far recovered approximately $11 million in illegal profits from the various defendants.

Matthew Bowin recruited investors for his company, *Interactive Products and Services*, in a direct public offering done entirely over the Internet. He raised $190,000 from 150 investors. But instead of using the money to build the company, Bowin pocketed the proceeds and bought groceries and stereo equipment. The SEC sued Bowin in a civil case, and the Santa Cruz, CA District Attorney's Office prosecuted him criminally. He was convicted of 54 felony counts and sentenced to 10 years in jail.

IVT Systems solicited investments to finance the construction of an ethanol plant in the Dominican Republic. The Internet solicitations promised a return of 50% or more with no reasonable basis for the prediction. Their literature contained lies about contracts with well known companies and omitted other important information for investors. After the SEC filed a complaint, they agreed to stop breaking the law.

Gene Block and Renate Haag were caught offering "prime bank" securities, a type of security that doesn't even exist. They collected over $3.5 million by promising to double investors' money in four months. The SEC has frozen their assets and stopped them from continuing their fraud.

Daniel Odulo was stopped from soliciting investors for a proposed eel farm. Odulo promised investors a "whopping 20% return," claiming that the investment was "low risk." When he was caught by the SEC, he consented to the court order stopping him from breaking the securities laws.

If you believe that you have been the victim of a securities-related fraud, through the Internet or otherwise, or if you believe that any person or entity may have violated or is currently violating the federal securities laws, you can submit a complaint using our online complaint form or email us at enforcement@sec.gov.

Be Alert for Telltale Signs of On-Line Investment Fraud

10 Questions To Ask About *Any* Investment Opportunity

INVESTigate Before You INVEST	Tips for Checking Out On-Line Newsletters

If you are aware of an online fraud, tell us about it!

http://www.sec.gov/investor/pubs/cyberfraud.htm

We have provided this information as a service to investors. It is neither a legal interpretation nor a statement of SEC policy. If you have questions concerning the meaning or application of a particular law or rule, please consult with an attorney who specializes in securities law.

Home | Previous Page

Modified: 08/06/2007

United States Government Accountability Office

GAO

Report to Congressional Committees

INFORMATION SECURITY

Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses

GAO

Accountability * Integrity * Reliability

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-09-546, a report to congressional committees

July 2009

INFORMATION SECURITY

Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses

Why GAO Did This Study

For many years, GAO has reported that weaknesses in information security are a widespread problem that can have serious consequences—such as intrusions by malicious users, compromised networks, and the theft of intellectual property and personally identifiable information—and has identified information security as a governmentwide high-risk issue since 1997.

Concerned by reports of significant vulnerabilities in federal computer systems, Congress passed the Federal Information Security Management Act of 2002 (FISMA), which authorized and strengthened information security program, evaluation, and reporting requirements for federal agencies.

In accordance with the FISMA requirement that the Comptroller General report periodically to Congress, GAO's objectives were to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) federal agencies' implementation of FISMA requirements. To address these objectives, GAO analyzed agency, inspectors general, Office of Management and Budget (OMB), and GAO reports.

What GAO Recommends

GAO is recommending that the Director of OMB take several actions, including revising guidance. OMB generally agreed with GAO's overall assessment of information security at agencies, but did not concur with one aspect of GAO's assessment of OMB's review activities.

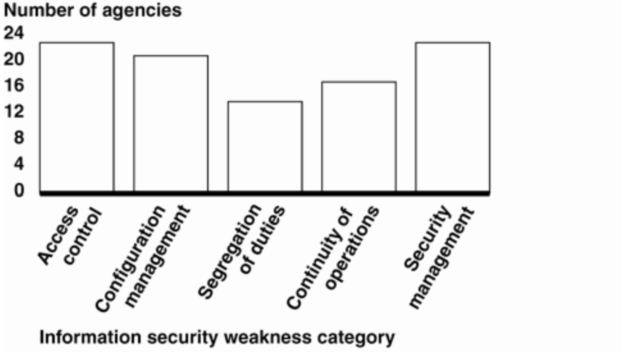
View GAO-09-546 or key components.
For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Persistent weaknesses in information security policies and practices continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of most federal agencies. Recently reported incidents at federal agencies have placed sensitive data at risk, including the theft, loss, or improper disclosure of personally identifiable information of Americans, thereby exposing them to loss of privacy and identity theft. For fiscal year 2008, almost all 24 major federal agencies had weaknesses in information security controls (see figure). An underlying reason for these weaknesses is that agencies have not fully implemented their information security programs. As a result, agencies have limited assurance that controls are in place and operating as intended to protect their information resources, thereby leaving them vulnerable to attack or compromise. In prior reports, GAO has made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls.

Federal agencies reported increased compliance in implementing key information security control activities for fiscal year 2008; however, inspectors general at several agencies noted shortcomings with agencies' implementation of information security requirements. Agencies reported increased implementation of control activities, such as providing awareness training for employees and testing system contingency plans. However, agencies reported decreased levels of testing security controls and training for employees who have significant security responsibilities. In addition, inspectors general at several agencies disagreed with performance reported by their agencies and identified weaknesses in the processes used to implement these activities. Further, although OMB took steps to clarify its reporting instructions to agencies for preparing fiscal year 2008 reports, the instructions did not request inspectors general to report on agencies' effectiveness of key activities and did not always provide clear guidance to inspectors general. As a result, the reporting may not adequately reflect agencies' implementation of the required information security policies and procedures.

Information Security Weaknesses at Major Federal Agencies for Fiscal Year 2008



Source: GAO analysis of IG, agency, and GAO reports.

Contents

Tables

Figures

Abbreviations

CD	compact disk
CIO	chief information officer
FISMA	Federal Information Security Management Act of 2002
IG	Inspector General
IP	Internet Protocol
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
US-CERT	U. S. Computer Emergency Readiness Team
US-VISIT	U. S. Visitor and Immigrant Status Indicator Technology

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 17, 2009

The Honorable Joseph I. Lieberman
Chairman
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security
and Governmental Affairs
United States Senate

The Honorable Edolphus Towns
Chairman
The Honorable Darrell Issa
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where the public's trust is essential. The need for a vigilant approach to information security is demonstrated by the increase in reports of security incidents, the wide availability of hacking tools, and steady advances in the sophistication and effectiveness of attack technology.

Over the past few years, 24 major federal agencies[1] have reported numerous security incidents in which sensitive information has been lost or stolen, including personally identifiable information, which has exposed millions of Americans to a loss of privacy, identity theft, and other

[1] The 24 major departments and agencies (agencies) are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

financial crimes. Since 1997, we have identified information security as a governmentwide high-risk issue in our biennial reports to Congress.[2]

Concerned by reports of significant weaknesses in federal computer systems, Congress passed the Federal Information Security Management Act (FISMA) of 2002,[3] which requires agencies to develop and implement an information security program, evaluation processes, and annual reporting. FISMA requires mandated annual reports by federal agencies, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). FISMA also includes a requirement for independent annual evaluations by the agencies' inspectors general or independent external auditors.

In accordance with the FISMA requirement that we report periodically to Congress, our objectives were to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) federal agencies' implementation of FISMA requirements. To accomplish these objectives, we analyzed agency, inspector general, OMB, and our reports on information security. Where possible, we categorized findings from those reports into areas defined by FISMA and the Federal Information System Controls Audit Manual.[4] We did not include systems categorized as national security systems in our review, nor did we review the adequacy or effectiveness of the security policies and practices for those systems.

We conducted this performance audit from December 2008 to May 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. For more details on our objectives, scope, and methodology, see appendix I.

[2] Most recently, GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

[3] FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

[4] GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: February 2009).

Background

Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain and manipulate sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. The risks to federal systems are well-founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology.

Recognizing the importance of securing federal systems and data, Congress passed FISMA in 2002. The act sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. FISMA's framework creates a cycle of risk management activities necessary for an effective security program; these activities are similar to the principles noted in our study of the risk management activities of leading private-sector organizations[5]—assessing risk, establishing a central management focal point, implementing appropriate policies and procedures, promoting awareness, and monitoring and evaluating policy and control effectiveness. In order to ensure the implementation of this framework, the act assigns specific responsibilities to agency heads, chief information officers, inspectors general, and NIST. It also assigns responsibilities to OMB that include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, and reviewing agency information security programs, at least annually, and approving or disapproving them.

Agency Responsibilities

FISMA requires each agency, including agencies with national security systems, to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Specifically, FISMA requires information security programs to include, among other things:

[5] GAO, *Executive Guide: Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;

- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;

- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;

- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;

- a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency;

- procedures for detecting, reporting, and responding to security incidents; and

- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

In addition, agencies must produce an annually updated inventory of major information systems (including major national security systems) operated by the agency or under its control, which includes an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency.

FISMA also requires each agency to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of its information security policies, procedures, practices, and compliance with requirements. In addition, agency heads are required to report annually the results of their independent evaluations to OMB, except to the extent that an evaluation pertains to a national security system; then only a summary and assessment of that portion of the evaluation needs to be reported to OMB.

Responsibilities of NIST

Under FISMA, NIST is tasked with developing, for systems other than national security systems, standards and guidelines that must include, at a minimum (1) standards to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security, according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category. NIST must also develop a definition of and guidelines for detection and handling of information security incidents as well as guidelines developed in conjunction with the Department of Defense and the National Security Agency for identifying an information system as a national security system.

The law also assigns other information security functions to NIST, including:

- providing technical assistance to agencies on elements such as compliance with the standards and guidelines and the detection and handling of information security incidents;
- evaluating private-sector information security policies and practices and commercially available information technologies to assess potential application by agencies;
- evaluating security policies and practices developed for national security systems to assess their potential application by agencies; and
- conducting research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security.

As required by FISMA, NIST has prepared its annual public report on activities undertaken in the previous year and planned for the coming year. In addition, NIST's FISMA initiative supports the development of a program for credentialing public and private sector organizations to provide security assessment services for federal agencies.

Responsibilities of Inspectors General

Under FISMA, the inspector general for each agency shall perform an independent annual evaluation of the agency's information security program and practices. The evaluation should include testing of the effectiveness of information security policies, procedures, and practices of a representative subset of agency systems. In addition, the evaluation must include an assessment of the compliance with the act and any related information security policies, procedures, standards, and guidelines. For agencies without an inspector general, evaluations of non-national security systems must be performed by an independent external auditor. Evaluations related to national security systems are to be performed by an entity designated by the agency head.

Responsibilities of OMB

FISMA states that the Director of OMB shall oversee agency information security policies and practices, including:

- developing and overseeing the implementation of policies, principles, standards, and guidelines on information security;
- requiring agencies to identify and provide information security protections commensurate with risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency, or information systems used or operated by an agency, or by a contractor of an agency, or other organization on behalf of an agency;
- overseeing agency compliance with FISMA to enforce accountability; and
- reviewing at least annually, and approving or disapproving, agency information security programs.

In addition, the act requires that OMB report to Congress no later than March 1 of each year on agency compliance with FISMA.

Weaknesses in Information Security Place Sensitive Information at Risk

Significant weaknesses in information security policies and practices threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of most federal agencies. These persistent weaknesses expose sensitive data to significant risk, as illustrated by recent incidents at various agencies. Further, our work and reviews by inspectors general note significant information security control deficiencies that place a broad array of federal operations and assets at risk. Consequently, we have made hundreds of recommendations to agencies to address these security control deficiencies.

Reported Incidents Are on the Rise and Place Sensitive Information at Risk

Since our report in July 2007, federal agencies have reported a spate of security incidents that have put sensitive data at risk, thereby exposing the personal information of millions of Americans to the loss of privacy and potential harm associated with identity theft. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices. The following examples, reported in 2008 and 2009, illustrate that a broad array of federal information and assets remain at risk.

- In May 2009, the Department of Transportation Inspector General issued the results of an audit of Web applications security and intrusion detection in air traffic control systems at the Federal Aviation Administration (FAA). The inspector general reported that Web applications used in supporting air traffic control systems operations were not properly secured to prevent attacks or unauthorized access. To illustrate, vulnerabilities found in Web application computers associated with the Traffic Flow Management Infrastructure System, Juneau Aviation Weather System, and the Albuquerque Air Traffic Control Tower allowed audit staff to gain unauthorized access to data stored on these computers, including program source code and sensitive personally identifiable information. In addition, the inspector general reported that it found a vulnerability on FAA Web applications that could allow attackers to execute malicious codes on FAA users' computers, which was similar to an actual incident that occurred in August 2008. In February 2009, the FAA notified employees that an agency computer had been illegally accessed and employee personal identity information had been stolen electronically. Two of the 48 files on the breached computer server contained personal information about more than 45,000 FAA employees and retirees who were on the FAA payrolls as of the first week of February 2006. Law enforcement agencies were notified and are investigating the data theft.

- In March 2009, U.S. Congressman Jason Altmire and U.S. Senator Bob Casey announced that that they had sent a letter to the Under Secretary of Defense for Acquisition, Technology, and Logistics, asking for additional information on a recent security breach of the presidential helicopter, Marine One. According to the announcement, in February 2009, a company based in Cranberry, Pennsylvania, discovered that engineering and communications documents containing key details about the Marine One fleet had been downloaded to an Internet Protocol (IP) address in Iran. The documents were traced back to a defense contractor in Maryland, where an employee most likely downloaded a file-sharing program that inadvertently allowed others to access this information. According to information from the Congressman's Web site, recent reports have said that the federal government was warned last June that an Internet Web site with an IP address traced to Iran was actively seeking this information.

- In March 2009, the United States Computer Emergency Readiness Team (US-CERT) issued an updated notice to warn agencies and organizations of the Conficker/Downadup worm activity and to help prevent further compromises from occurring. In the notice, US-CERT warned that the Conficker/Downadup worm could infect a Microsoft Windows system from a thumb drive, a network share, or directly across a network if the host is not patched.

- According to a March 2009 media release from Senator Bill Nelson's office, cyber-invaders thought to be in China hacked into the computer network in Senator Nelson's office. There were two attacks on the same day in March 2009, and another one in February 2009 that targeted work stations used by three of Senator Nelson's staffers. The hackers were not able to take any classified information because that information is not kept on office computers, a spokesman said. The media release stated that similar incursions into computer networks in Congress were up significantly in the past few months.

- The Department of Energy's Office of Health, Safety, and Security announced that a password-protected compact disk (CD) had been lost during a routine shipment on January 28, 2009. The CD contained personally identifiable information for 59,617 individuals who currently work or formerly worked at facilities at the Department of Energy's Idaho site. The investigation verified that protection measures had been applied in accordance with requirements applicable to organizations working under cooperative agreements and surmised that while the CD had been lost for 8 weeks at the time of the investigation, no evidence had been found that revealed that the personal information on the lost disk had been compromised. The investigation concluded that OMB and Department of Energy requirements for managing and reporting the loss of the information had not been transmitted to the appropriate organizations and that there was a failure to provide timely notifications of the actual or suspected loss of information in this incident.

- In January 2009, the Program Director of the Office of Personnel and Management's USAJOBS Web site announced that their technology provider's (Monster.com) database had been illegally accessed and contact and account data had been taken, including user IDs and passwords, e-mail addresses, names, phone numbers, and some basic demographic data. The director pointed out that e-mail could be used for phishing activity and advised users to change their site login password.

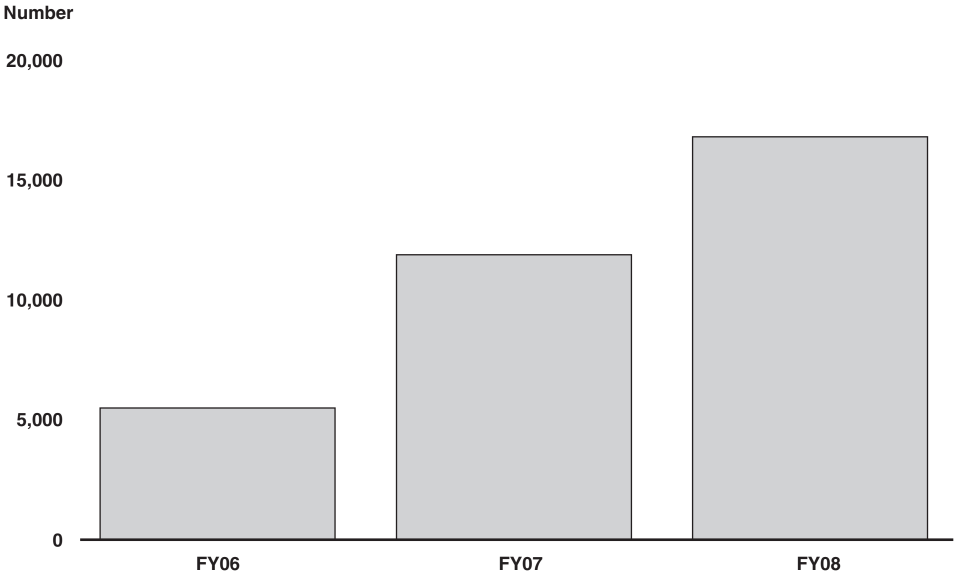
- In December 2008, the Federal Emergency Management Administration was alerted to an unauthorized breach of private information when an applicant notified it that his personal information pertaining to Hurricane Katrina had been posted on the Internet. The information posted to Web sites contained a spreadsheet with 16,857 lines of data that included applicant names, social security numbers, addresses, telephone numbers, e-mail addresses, and other information on disaster applicants who had evacuated to Texas. According to the Federal Emergency Management Administration, it took action to work with the Web site hosting the private information, and have that information removed from public view. Additionally, the agency reported that it worked to remove the same information from a second Web site. Further, the agency stated that while it believed most of the applicant information posted on the Web sites were properly released by them to a state agency, it did not authorize the subsequent public posting of much of this data.

- In June 2008, the Walter Reed Army Medical Center reported that officials were investigating the possible disclosure of personally identifiable information through unauthorized sharing of a data file containing the names of approximately 1,000 Military Health System beneficiaries. Walter Reed officials were notified of the possible exposure on May 21 by an outside company. Preliminary results of an ongoing investigation identified a computer from which the data had apparently been compromised. Data security personnel from Walter Reed and the Department of the Army think it is possible that individuals named in the file could become victims of identity theft. The compromised data file did not include protected health information such as medical records, diagnosis, or prognosis for patients.

- In March 2008, media reports surfaced noting that the passport files of three U.S. senators, who were also presidential candidates, had been improperly accessed by Department of State employees and contractor staff. As of April 2008, the system contained records on about 192 million passports for about 127 million passport holders. These records included personally identifiable information, such as the applicant's name, gender, social security number, date and place of birth, and passport number. In July 2008, after investigating this incident, the Department of State's Office of Inspector General reported many control weaknesses—including a general lack of policies, procedures, guidance, and training—relating to the prevention and detection of unauthorized access to passport and applicant information and the subsequent response and disciplinary processes when a potential unauthorized access is substantiated.

When incidents occur, agencies are to notify the federal information security incident center—US-CERT. As shown in figure 1, the number of incidents reported by federal agencies to US-CERT has risen dramatically over the past 3 years, increasing from 5,503 incidents reported in fiscal year 2006 to 16,843 incidents in fiscal year 2008 (slightly more than 200 percent).

Figure 1: Incidents Reported to US-CERT, FY 2006-FY 2008



Source: GAO analysis of US-CERT data.

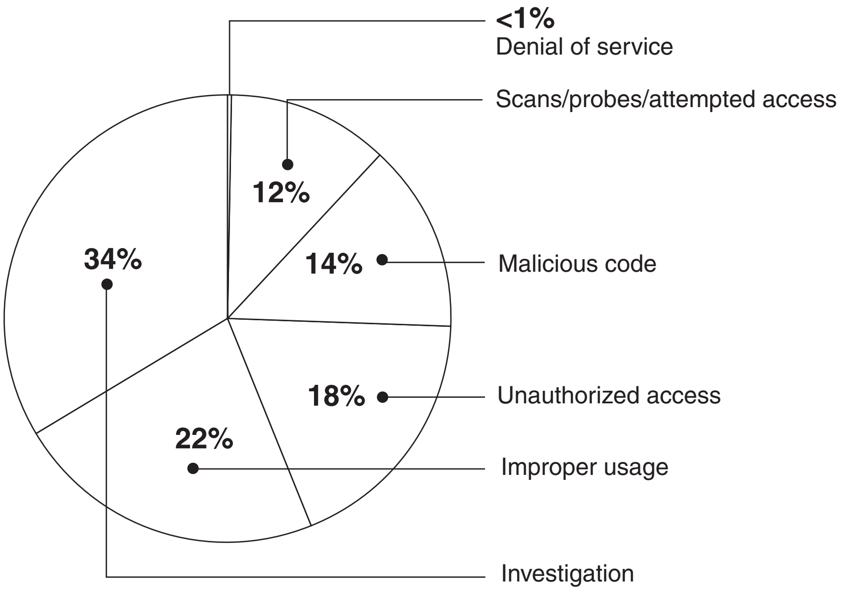
Agencies report the following types of incidents based on US-CERT-defined categories:

- **Unauthorized access:** Gaining logical or physical access without permission to a federal agency's network, system, application, data, or other resource.
- **Denial of service:** Preventing or impairing the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim of or participating in a denial of service attack.
- **Malicious code:** Installing malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus software.
- **Improper usage:** Violating acceptable computing use policies.
- **Scans/probes/attempted access:** Accessing or identifying a federal agency computer, open ports, protocols, service, or any combination of these for later exploit. This activity does not directly result in a compromise or denial of service.

Under investigation: Investigating unconfirmed incidents that are potentially malicious, or anomalous activity deemed by the reporting entity to warrant further review.

As noted in figure 2, the three most prevalent types of incidents reported to US-CERT during fiscal years 2006 through 2008 were unauthorized access, improper usage, and investigation (see fig. 2).

Figure 2: Percentage of Incidents Reported to US-CERT in FY06-FY08 by Category



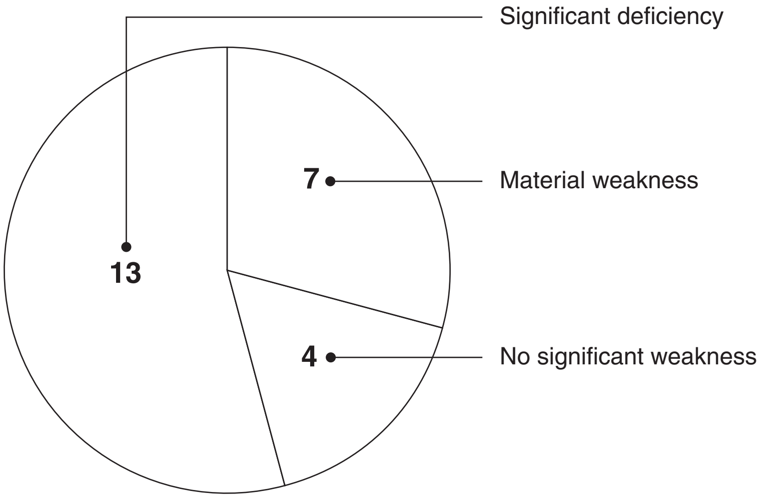
Source: GAO analysis of US-CERT data.

Weaknesses in Controls Highlight Deficiencies in the Implementation of Security Policies and Practices

Reviews at federal agencies continue to highlight deficiencies in their implementation of security policies and procedures. In their fiscal year 2008 performance and accountability reports, 20 of the 24 agencies indicated that inadequate information security controls were either a material weakness or a significant deficiency[6] (see fig. 3).

[6] A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

Figure 3: Number of Major Agencies Reporting Significant Deficiencies in Information Security



Source: GAO analysis of agency performance and accountability reports for FY 2008.

Similarly, in annual reports required under 31 U.S.C. § 3512 (commonly referred to as the *Federal Managers' Financial Integrity Act of 1982*),[7] 11 of 24 agencies identified material weaknesses in information security. Inspectors general have also noted weaknesses in information security, with 22 of 24 identifying it as a "major management challenge" for their agency.[8]

Similarly, our audits have identified control deficiencies in both financial and nonfinancial systems, including vulnerabilities in critical federal systems. For example:

[7] FMFIA, Pub. L. No. 97-255, 96 Stat. 814 (Sept. 8, 1982), now codified at 31 U.S.C. § 3512, requires agencies to report annually to the President and Congress on the effectiveness of internal controls and any identified material weaknesses in those controls. Per OMB, for the purposes of FMFIA reporting, a material weakness also encompasses weaknesses found in program operations and compliance with applicable laws and regulations. Material weaknesses for FMFIA reporting are determined by management, whereas material weaknesses reported as part of a financial statement audit are determined by independent auditors.

[8] The Reports Consolidation Act of 2000, Pub. L. No. 106-531, 114 Stat. 2537 (Nov. 22, 2000), requires inspectors general to include in their agencies' performance and accountability reports a statement that summarizes what they consider to be the most serious management and performance challenges facing their agencies and briefly assesses their agencies' progress in addressing those challenges. 31 U.S.C. § 3516(d).

- In 2009, we reported that security weaknesses at the Securities and Exchange Commission continued to jeopardize the confidentiality, integrity, and availability of the commission's financial and sensitive information and information systems.[9] Although the commission had made progress in correcting previously reported information security control weaknesses, it had not completed action to correct 16 weaknesses. In addition, we identified 23 new weaknesses in controls intended to restrict access to data and systems. Thus, the commission had not fully implemented effective controls to prevent, limit, or detect unauthorized access to computing resources. For example, it had not always (1) consistently enforced strong controls for identifying and authenticating users, (2) sufficiently restricted user access to systems, (3) encrypted network services, (4) audited and monitored security-relevant events for its databases, and (5) physically protected its computer resources. The Securities and Exchange Commission also had not consistently ensured appropriate segregation of incompatible duties or adequately managed the configuration of its financial information systems. As a result, the Securities and Exchange Commission was at increased risk of unauthorized access to and disclosure, modification, or destruction of its financial information, as well as inadvertent or deliberate disruption of its financial systems, operations, and services. The Securities and Exchange Commission agreed with our recommendations and stated that it plans to address the identified weaknesses.

- In 2009, we reported that the Internal Revenue Service had made progress toward correcting prior information security weaknesses, but continued to have weaknesses that could jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information.[10] These deficiencies included some related to controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities, as well as a control important in mitigating software vulnerability risks. For example, the agency continued to, among other things, allow sensitive information, including IDs and passwords for mission-critical applications, to be readily available to any user on its internal network and to grant excessive access to individuals who do not need it. In addition, the Internal Revenue Service had systems running unsupported software that could not be patched against known

[9] GAO, *Information Security: Securities and Exchange Commission Needs to Consistently Implement Effective Controls*, GAO-09-203 (Washington, D.C.: Mar. 16, 2009).

[10] GAO, *Information Security: Continued Efforts Needed to Address Significant Weaknesses at IRS*, GAO-09-136 (Washington, D.C.: Jan. 9, 2009).

vulnerabilities. Until those weaknesses are corrected, the Internal Revenue Service remains vulnerable to insider threats and is at increased risk of unauthorized access to and disclosure, modification, or destruction of financial and taxpayer information, as well as inadvertent or deliberate disruption of system operations and services. The IRS agreed to develop a plan addressing each of our recommendations.

- In 2008, we reported that although the Los Alamos National Laboratory—one of the nation's weapons laboratories—implemented measures to enhance the information security of its unclassified network, vulnerabilities continued to exist in several critical areas, including (1) identifying and authenticating users of the network, (2) encrypting sensitive information, (3) monitoring and auditing compliance with security policies, (4) controlling and documenting changes to a computer system's hardware and software, and (5) restricting physical access to computing resources.[11] As a result, sensitive information on the network—including unclassified controlled nuclear information, naval nuclear propulsion information, export control information, and personally identifiable information—were exposed to an unnecessary risk of compromise. Moreover, the risk was heightened because about 300 (or 44 percent) of 688 foreign nationals who had access to the unclassified network as of May 2008 were from countries classified as sensitive by the Department of Energy, such as China, India, and Russia. While the organization did not specifically comment on our recommendations, it agreed with the conclusions.

- In 2008, we reported that the Tennessee Valley Authority had not fully implemented appropriate security practices to secure the control systems used to operate its critical infrastructures at facilities we reviewed.[12] Multiple weaknesses within the Tennessee Valley Authority corporate network left it vulnerable to potential compromise of the confidentiality, integrity, and availability of network devices and the information transmitted by the network. For example, almost all of the workstations and servers that we examined on the corporate network lacked key security patches or had inadequate security settings. Furthermore,

[11] GAO, *Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network*, GAO-08-1001 (Washington, D.C.: Sept. 9, 2008).

[12] GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, GAO-08-526 (Washington, D.C.: May 21, 2008) and *Information Security: TVA Needs to Enhance Security of Critical Infrastructure Controls Systems and Networks*, GAO-08-755T (Washington, D.C.: May 21, 2008).

Tennessee Valley Authority had not adequately secured its control system networks and devices on these networks, leaving the control systems vulnerable to disruption by unauthorized individuals. In addition, we reported that the network interconnections provided opportunities for weaknesses on one network to potentially affect systems on other networks. Specifically, weaknesses in the separation of network segments could allow an individual who had gained access to a computing device connected to a less secure portion of the network to be able to compromise systems in a more secure portion of the network, such as the control systems. As a result, Tennessee Valley Authority's control systems were at increased risk of unauthorized modification or disruption by both internal and external threats and could affect its ability to properly generate and deliver electricity. The Tennessee Valley Authority agreed with our recommendations and provided information on steps it was taking to implement them.

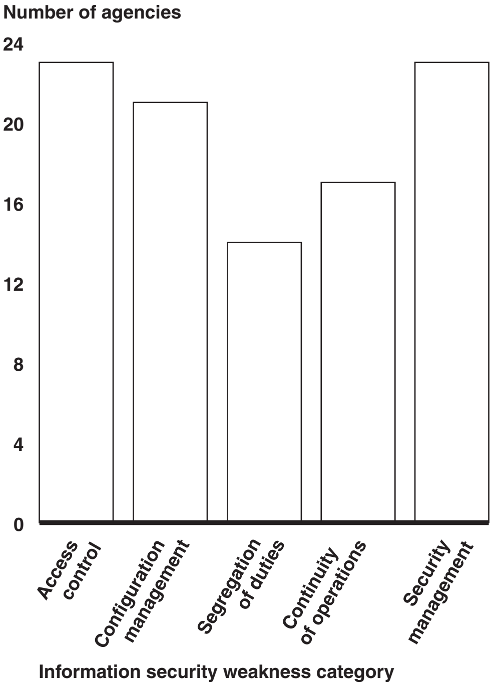
- In 2007, we reported that the Department of Homeland Security had significant weaknesses in computer security controls surrounding the information systems used to support its U.S. Visitor and Immigrant Status Technology (US-VISIT) program for border security.[13] For example, it had not implemented controls to effectively prevent, limit, and detect access to computer networks, systems, and information. Specifically, it had not (1) adequately identified and authenticated users in systems supporting US-VISIT; (2) sufficiently limited access to US-VISIT information and information systems; (3) ensured that controls adequately protected external and internal network boundaries; (4) effectively implemented physical security at several locations; (5) consistently encrypted sensitive data traversing the communication network; and (6) provided adequate logging or user accountability for the mainframe, workstations, or servers. In addition, it had not always ensured that responsibilities for systems development and system production had been sufficiently segregated and had not consistently maintained secure configurations on the application servers and workstations at a key data center and ports of entry. As a result, increased risk existed that unauthorized individuals could read, copy, delete, add, and modify sensitive information—including personally identifiable information—and disrupt service on Customs and Border Protection systems supporting the US-VISIT program. The department stated that it directed Customs and Border Protection to complete remediation activities to address each of our recommendations.

[13] GAO, *Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program*, GAO-07-870 (Washington, D.C.: July 13, 2007).

Weaknesses Persist in All Major Categories of Controls

According to our reports and those of agency inspectors general, persistent weaknesses appear in the five major categories of information system controls: (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and (5) an agencywide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented. Most agencies continue to have weaknesses in each of these categories, as shown in figure 4.

Figure 4: Information Security Weaknesses at 24 Major Agencies for FY 2008



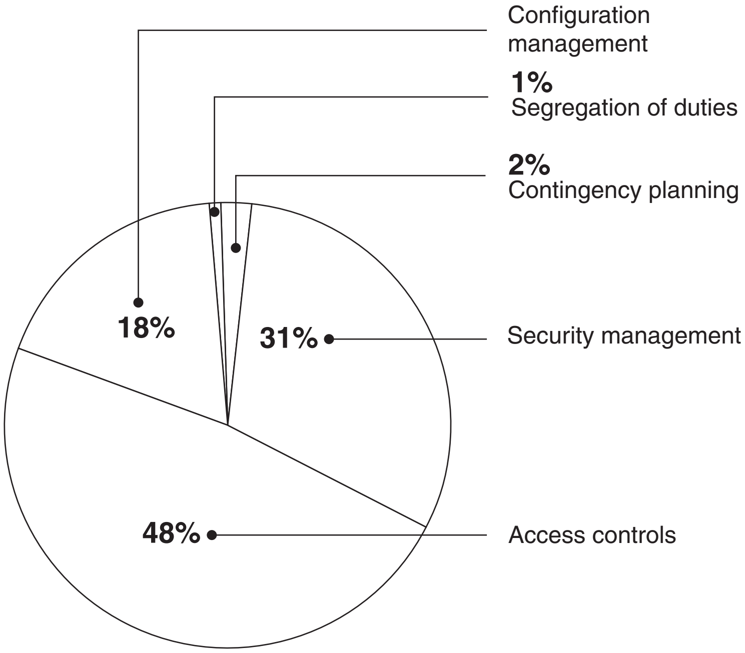
Source: GAO analysis of IG, agency, and GAO reports.

Access Controls Were Not Adequate

Agencies use access controls to limit, prevent, or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized use, modification, disclosure, and loss. Such controls include both electronic and physical controls. Electronic access controls include those related to boundary protection, user identification and authentication, authorization, cryptography, and auditing and monitoring. Physical access controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls involve restricting physical access to computer resources, usually by limiting access to the buildings and rooms in which they are housed and enforcing usage restrictions and implementation guidance for portable and mobile devices.

At least 23 major federal agencies had access control weaknesses during fiscal year 2008. An analysis of our reports reveals that 48 percent of information security control weaknesses pertained to access controls (see fig. 5). For example, agencies did not consistently (1) establish sufficient boundary protection mechanisms; (2) identify and authenticate users to prevent unauthorized access; (3) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (4) apply encryption to protect sensitive data on networks and portable devices; (5) log, audit, and monitor security-relevant events; and (6) establish effective controls to restrict physical access to information assets. Without adequate access controls in place, agencies cannot ensure that their information resources are protected from intentional or unintentional harm.

Figure 5: Control Weaknesses Identified in GAO Reports, May 2007-April 2009



Source: GAO analysis of prior GAO reports.

Boundary Protection

Boundary protection controls logical connectivity into and out of networks and controls connectivity to and from network connected devices. Agencies segregate the parts of their networks that are publicly accessible by placing these components in subnetworks with separate physical interfaces and preventing public access to their internal networks. Unnecessary connectivity to an agency's network increases not only the number of access paths that must be managed and the complexity of the task, but the risk of unauthorized access in a shared environment. In addition to deploying a series of security technologies at multiple layers, deploying diverse technologies at different layers helps to mitigate the risk of successful cyber attacks. For example, multiple firewalls can be deployed to prevent both outsiders and trusted insiders from gaining unauthorized access to systems, and intrusion detection technologies can be deployed to defend against attacks from the Internet.

Agencies continue to demonstrate vulnerabilities in establishing appropriate boundary protections. For example, two agencies that we assessed did not adequately secure channels to connect remote users, increasing the risk that attackers will use these channels to gain access to restricted network resources. One of these agencies also did not have adequate intrusion detection capabilities, while the other allowed users of one network to connect to another, higher-security network. Such weaknesses in boundary protections impair an agency's ability to deflect and detect attacks quickly and protect sensitive information and networks.

User Identification and Authentication

A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals. When an organization assigns unique user accounts to specific users, the system is able to distinguish one user from another—a process called identification. The system also must establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication.

Agencies did not always adequately control user accounts and passwords to ensure that only valid users could access systems and information. In our 2007 FISMA report,[14] we noted several weaknesses in agencies' identification and authentication procedures. Agencies continue to experience similar weaknesses in fiscal years 2008 and 2009. For example, certain agencies did not adequately enforce strong password settings, increasing the likelihood that accounts could be compromised and used by unauthorized individuals to gain access to sensitive information. In other instances, agencies did not enforce periodic changing of passwords or use of one-time passwords or passcodes, and transmitted or stored passwords in clear text. Poor password management increases the risk that unauthorized users could guess or read valid passwords to devices and use the compromised devices for an indefinite period of time.

Authorization

Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. A key component of granting or denying access rights is the concept of least privilege, which is a basic principle for

[14] GAO, *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, GAO-07-837 (Washington, D.C.: July 27, 2007).

securing computer resources and information and means that users are granted only those access rights and permissions that they need to perform their official duties. To restrict legitimate users' access to only those programs and files that they need to do their work, agencies establish access rights and permissions. "User rights" are allowable actions that can be assigned to users or to groups of users. File and directory permissions are rules that regulate which users can access a particular file or directory and the extent of that access. To avoid unintentionally authorizing users access to sensitive files and directories, an agency must give careful consideration to its assignment of rights and permissions.

Agencies continued to grant rights and permissions that allowed more access than users needed to perform their jobs. Inspectors general at 12 agencies reported instances where users had been granted excessive privileges. In our reviews, we also noted vulnerabilities in this area. For example, at one agency, users could inappropriately escalate their access privileges to run commands on a powerful system account, many had unnecessary and inappropriate access to databases, and other accounts allowed excessive privileges and permissions. Another agency allowed (on financial applications) generic, shared accounts that included the ability to create, delete, and modify users' accounts. Approximately 1,100 users at yet another agency had access to mainframe system management utilities, although such access was not necessarily required to perform their jobs. These utilities provided access to all files stored on disk; all programs running on the system, including the outputs; and the ability to alter hardware configurations supporting the production environment. We uncovered one agency that had provided a contractor with system access that was beyond what was needed, making the agency vulnerable to incidents on the contractor's network. Another agency gave all users of an application full access to the application's source code although their responsibilities did not require this level of privilege. Such weaknesses in authorization place agencies at increased risk of inappropriate access to data and sensitive system programs, as well as to the consequent disruption of services.

Cryptography

Cryptography[15] underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. A basic element of cryptography is encryption. Encryption can be used to provide basic data confidentiality and integrity by transforming plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm. The National Security Agency recommends disabling protocols that do not encrypt information transmitted across the network, such as user identification and password combinations.

Agencies did not always encrypt sensitive information on their systems or traversing the network. In our reviews of agencies' information security, we found that agencies did not always encrypt sensitive information. For example, five agencies that we reviewed did not effectively use cryptographic controls to protect sensitive resources. Specifically, one agency allowed unencrypted protocols to be used on its network devices. Another agency did not require encrypted passwords for network logins, while another did not consistently provide approved, secure transmission of data over its network. These weaknesses could allow an attacker, or malicious user, to view information and use that knowledge to obtain sensitive financial and system data being transmitted over the network.

Auditing and Monitoring

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine what, when, and by whom specific actions have been taken on a system. Agencies accomplish this by implementing system or security software that provides an audit trail, or logs of system activity, that they can use to determine the source of a transaction or attempted transaction and to monitor users' activities. The way in which agencies configure system or security software determines the nature and extent of the information that can be provided by the audit trail. To be effective, agencies should configure their software to collect and maintain audit trails that are sufficient to track security-relevant events.

[15] Cryptography is used to secure transactions by providing ways to ensure data confidentiality, data integrity, authentication of the message's originator, electronic certification of data, and nonrepudiation (proof of the integrity and origin of data that can be verified by a third party).

Agencies did not sufficiently log and monitor key security- and audit-related events on their network. For example, agencies did not monitor critical portions of their networks for intrusions; record successful, unauthorized access attempts; log certain changes to data on a mainframe (which increases the risk of compromised security controls or disrupted operations); and capture all authentication methods and logins to a network by foreign nationals. Similarly, 14 agencies did not always have adequate auditing and monitoring capabilities. For example, one agency did not conduct a baseline assessment of an important network. This baseline determines a typical state or pattern of network activity. Without this information, the agency could have difficulty detecting and investigating anomalous activity to ascertain whether or not an attack was under way. Another agency did not perform source code scanning or have a process for manual source code reviews, which increases the risk that vulnerabilities would not be detected. As a result, unauthorized access could go undetected, and if a system is modified or disrupted, the ability to trace or recreate events could be impeded.

Physical Security

Physical security controls help protect computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to sensitive computing and communications resources, usually by limiting access to the buildings and rooms in which the resources are housed. Examples of physical security controls include perimeter fencing, surveillance cameras, security guards, locks, and procedures for granting or denying individuals physical access to computing resources. Physical controls also include environmental controls such as smoke detectors, fire alarms, extinguishers, and uninterruptible power supplies. Considerations for perimeter security also include controlling vehicular and pedestrian traffic. In addition, visitors' access to sensitive areas must be managed appropriately.

Our analysis of inspector general, GAO, and agency reports has shown that nine agencies did not sufficiently restrict physical access to sensitive computing and communication resources. The physical security measures employed by these agencies often did not comply with their own requirements or with federal standards. Access to facilities containing sensitive equipment and information was not always adequately restricted. For example, at one agency with buildings housing classified networks, cars were not stopped and inspected; a sign indicated the building's purpose; fencing was scalable; and access to buildings containing computer network equipment was not controlled by electronic or other means. Agencies did not adequately manage visitors, in one instance, placing network jacks in an area where unescorted individuals could use them to obtain electronic access to restricted computing resources, and in another failing to properly identify and control visitors at a facility containing sensitive equipment. Agencies did not always remove employees' physical access authorizations to sensitive areas in a timely manner when they departed or their work no longer required such access. Environmental controls at one agency did not meet federal guidelines, with fire suppression capabilities, emergency lighting, and backup power all needing improvements. Such weaknesses in physical access controls increase the risk that sensitive computing resources will inadvertently or deliberately be misused, damaged, or destroyed.

Configuration Management Controls Were Not Always Implemented

Configuration management controls ensure that only authorized and fully tested software is placed in operation. These controls, which also limit and monitor access to powerful programs and sensitive files associated with computer operations, are important in providing reasonable assurance that access controls are not compromised and that the system will not be impaired. These policies, procedures, and techniques help ensure that all programs and program modifications are properly authorized, tested, and approved. Further, patch management is an important element in mitigating the risks associated with software vulnerabilities. Up-to-date patch installation could help mitigate vulnerabilities associated with flaws in software code that could be exploited to cause significant damage—including the loss of control of entire systems—thereby enabling malicious individuals to read, modify, or delete sensitive information or disrupt operations.

Twenty-one agencies demonstrated weaknesses in configuration management controls. For instance, several agencies did not implement common secure configuration policies across their systems, increasing the risk of avoidable security vulnerabilities. In addition, agencies did not effectively ensure that system software changes had been properly authorized, documented, and tested, which increases the risk that unapproved changes could occur without detection and that such changes could disrupt a system's operations or compromise its integrity. Agencies did not always monitor system configurations to prevent extraneous services and other vulnerabilities from remaining undetected and jeopardizing operations. At least six agencies did not consistently update software on a timely basis to protect against known vulnerabilities or did not fully test patches before applying them. Without a consistent approach to updating, patching, and testing software, agencies are at increased risk of exposing critical and sensitive data to unauthorized and possibly undetected access.

Segregation of Duties Was Not Appropriately Enforced

Segregation of duties refers to the policies, procedures, and organizational structure that helps ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records. Proper segregation of duties is achieved by dividing responsibilities among two or more individuals or groups. Dividing duties among individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one individual or group will serve as a check on the activities of the other.

At least 14 agencies did not appropriately segregate information technology duties. These agencies generally did not assign employee duties and responsibilities in a manner that segregated incompatible functions among individuals or groups of individuals. For instance, at one agency, an individual who enters an applicant's data into a financial system also had the ability to hire the applicant. At another agency, 76 system users had the ability to create and approve purchase orders. Without adequate segregation of duties, there is an increased risk that erroneous or fraudulent actions can occur, improper program changes can be implemented, and computer resources can be damaged or destroyed.

Continuity of Operations Plans Have Shortcomings

An agency must take steps to ensure that it is adequately prepared to cope with the loss of operational capabilities due to an act of nature, fire, accident, sabotage, or any other disruption. An essential element in preparing for such a catastrophe is an up-to-date, detailed, and fully tested continuity of operations plan. Such a plan should cover all key computer operations and should include planning to ensure that critical information systems, operations, and data such as financial processing and related records can be properly restored if an emergency or a disaster occurs. To ensure that the plan is complete and fully understood by all key staff, it should be tested— including unannounced tests—and test plans and results documented to provide a basis for improvement. If continuity of operations controls are inadequate, even relatively minor interruptions could result in lost or incorrectly processed data, which could cause financial losses, expensive recovery efforts, and inaccurate or incomplete mission-critical information.

Although agencies have reported increases in the number of systems for which contingency plans have been tested, at least 17 agencies had shortcomings in their continuity of operations plans. For example, one agency's disaster recovery planning had not been completed. Specifically, disaster recovery plans for three components of the agency were in draft form and had not been tested. Another agency did not include a business impact analysis in the contingency plan control, which would assist in planning for system recovery. In another example, supporting documentation for some of the functional tests at the agency did not adequately support testing results for verifying readability of backup tapes retrieved during the tests. Until agencies complete actions to address these weaknesses, they are at risk of not being able to appropriately recover systems in a timely manner from certain service disruptions.

Agencywide Security Programs Were Not Fully Implemented

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented agencywide information security programs. An agencywide security program, as required by FISMA, provides a framework and continuing cycle of activity for assessing and managing risk, developing and implementing security policies and procedures, promoting security awareness and training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources.

Twenty-three agencies had not fully or effectively implemented agencywide information security programs. Agencies often did not adequately design or effectively implement policies for elements key to an information security program. Weaknesses in agency information security program activities, such as risk assessments, information security policies and procedures, security planning, security training, system testing and evaluation, and remedial action plans are described next.

Risk Assessments

In order for agencies to determine what security controls are needed to protect their information resources, they must first identify and assess their information security risks. Moreover, by increasing awareness of risks, these assessments can generate support for policies and controls.

Agencies have not fully implemented their risk assessment processes. In addition, 14 major agencies had weaknesses in their risk assessments. Furthermore, they did not always properly assess the impact level of their systems or evaluate potential risks for the systems we reviewed. For example, one agency had not yet finalized and approved its guidance for completing risk assessments. In another example, the agency had not properly categorized the risk to its system, because it had performed a risk assessment without an inventory of interconnections to other systems. Similarly, another agency had not completed risk assessments for its critical systems and had not assigned impact levels. In another instance, an agency had current risk assessments that documented residual risk assessed and potential threats, and recommended corrective actions for reducing or eliminating the vulnerabilities they had identified. However, that agency had not identified many of the vulnerabilities we found and had not subsequently assessed the risks associated with them. As a result of these weaknesses, agencies may be implementing inadequate or inappropriate security controls that do not address the systems' true risk, and potential risks to these systems may not be known.

Policies and Procedures

According to FISMA, each federal agency's information security program must include policies and procedures that are based on risk assessments that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each agency's information system. The term 'security policy' refers to specific security rules set up by the senior management of an agency to create a computer security program, establish its goals, and assign responsibilities. Because policy is written at a broad level, agencies also develop standards, guidelines, and procedures that offer managers, users, and others a clear approach to implementing policy and meeting organizational goals.

Thirteen agencies had weaknesses in their information security policies and procedures. For example, one agency did not have updated policies and procedures for configuring operating systems to ensure they provide the necessary detail for controlling and logging changes. Another agency had not established adequate policies or procedures to implement and maintain an effective departmentwide information security program or to address key OMB privacy requirements. Agencies also exhibited weaknesses in policies concerning security requirements for laptops, user access privileges, security incidents, certification and accreditation, and physical security. As a result, agencies have reduced assurance that their systems and the information they contain are sufficiently protected. Without policies and procedures that are based on risk assessments, agencies may not be able to cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each agency's information system.

Security Plans

FISMA requires each federal agency to develop plans for providing adequate information security for networks, facilities, and systems or groups of systems. According to NIST 800-18, system security planning is an important activity that supports the system development life cycle and should be updated as system events trigger the need for revision in order to accurately reflect the most current state of the system. The system security plan provides a summary of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. NIST guidance also indicates that all security plans should be reviewed and updated, if appropriate, at least annually. Further, appendix III of OMB Circular A-130 requires security plans to include controls for, among other things, contingency planning and system interconnections.

System security plans were incomplete or out of date at several agencies. For example, one agency had an incomplete security plan for a key application. Another agency had only developed a system security plan that covered two of the six facilities we reviewed, and the plan was incomplete and not up-to-date. At another agency, 52 of the 57 interconnection security agreements listed in the security plan were not current since they had not been updated within 3 years. Without adequate security plans in place, agencies cannot be sure that they have the appropriate controls in place to protect key systems and critical information.

Specialized Training

Users of information resources can be one of the weakest links in an agency's ability to secure its systems and networks. Therefore, an important component of an agency's information security program is providing the required training so that users understand system security risks and their own role in implementing related policies and controls to mitigate those risks.

Several agencies had not ensured that all information security employees and contractors, including those who have significant information security responsibilities, had received sufficient training. For example, users of one agency's IT systems had not been trained to check for continued functioning of their encryption software after installation. At another agency, officials stated that several of its components had difficulty in identifying and tracking all employees who have significant IT security responsibilities and thus were unable to ensure that they received the specialized training necessary to effectively perform their responsibilities. Without adequate training, users may not understand system security risks and their own role in implementing related policies and controls to mitigate those risks.

System Tests and Evaluations

Another key element of an information security program is testing and evaluating system controls to ensure that they are appropriate, effective, and comply with policies. FISMA requires that agencies test and evaluate the information security controls of their major systems and that the frequency of such tests be based on risk, but occur no less than annually. NIST requires agencies to ensure that the appropriate officials are assigned roles and responsibilities for testing and evaluating controls over their systems.

Agencies did not always implement policies and procedures for performing periodic testing and evaluation of their information security controls. For example, one agency had not adequately tested security controls. Specifically, the tests of a major application and the mainframe did not identify or discuss the vulnerabilities that we had identified during our audit. The same agency’s testing did not reveal problems with the mainframe that could allow unauthorized users to read, copy, change, delete, and modify data. In addition, although testing requirements were stated in test documentation, the breadth and depth of the test, as well as the results of the test, had not always been documented. Also, agencies reported inconsistent testing of security controls among components. Without conducting the appropriate tests and evaluations, agencies have limited assurance that policies and controls are appropriate and working as intended. Additionally, there is an increased risk that undetected vulnerabilities could be exploited to allow unauthorized access to sensitive information.

Remedial Action Processes and Plans

FISMA requires that agencies’ information security programs include a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency.

Since our 2007 FISMA report, we have continued to find weaknesses in agencies' plans and processes for remedial actions. Agencies indicated that they had corrected or mitigated weaknesses; however, our work revealed that those weaknesses still existed. In addition, the inspectors general at 14 of the 24 agencies reported weaknesses in the plans to document remedial actions. For example, at several agencies, the inspector general reported that weaknesses had been identified but not documented in the remediation plans. Inspectors general further reported that agency plans did not include all relevant information in accordance with OMB instructions. We also found that deficiencies had not been corrected in a timely manner. Without a mature process and effective remediation plans, the risk increases that vulnerabilities in agencies' systems will not be mitigated in an effective and timely manner.

Until agencies effectively and fully implement agencywide information security programs, federal data and systems will not be adequately safeguarded to prevent disruption, unauthorized use, disclosure, and modification. Further, until agencies implement our recommendations to correct specific information security control weaknesses, their systems and information will remain at increased risk of attack or compromise.

Opportunities Exist for Bolstering Federal Information Security

In prior reports,[16] we and inspectors general have made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls. For example, we recommended that agencies correct specific information security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, and continuity of operations planning. We have also recommended that agencies fully implement comprehensive, agencywide information security programs by correcting weaknesses in risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. The effective implementation of these recommendations will strengthen the security posture at these agencies. Agencies have implemented or are in the process of implementing many of our recommendations.

[16] See related GAO products for a list of our recent reports on information security.

In March 2009, we reported on 12 key improvements suggested by a panel of experts as being essential to improving our national cyber security posture (see app. III).[17] The expert panel included former federal officials, academics, and private-sector executives. Their suggested improvements are intended to address many of the information security vulnerabilities facing both private and public organizations, including federal agencies. Among these improvements are recommendations to develop a national strategy that clearly articulates strategic objectives, goals, and priorities and to establish a governance structure for strategy implementation.

Due to increasing cyber security threats, the federal government has initiated several efforts to protect federal information and information systems. Recognizing the need for common solutions to improving security, the White House, OMB, and federal agencies have launched or continued several governmentwide initiatives that are intended to enhance information security at federal agencies. These key initiatives are discussed here.

- *60-day cyber review:* The National Security Council and Homeland Security Council recently completed a 60-day interagency review intended to develop a strategic framework to ensure that federal cyber security initiatives are appropriately integrated, resourced, and coordinated with Congress and the private sector. The resulting report recommended, among other things, appointing an official in the White House to coordinate the nation's cybersecurity policies and activities, creating a new national cybersecurity strategy, and developing a framework for cyber research and development.[18]

- *Comprehensive National Cybersecurity Initiative:* In January 2008, President Bush began to implement a series of initiatives aimed primarily at improving the Department of Homeland Security and other federal agencies' efforts to protect against intrusion attempts and anticipate future threats.[19] While these initiatives have not been made public, the Director of National Intelligence stated that they include defensive, offensive,

[17] GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, GAO-09-432T (Washington, D.C.: Mar. 10, 2009).

[18] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

[19] The White House, *National Security Presidential Directive 54/ Homeland Security Presidential Directive 23* (Washington, D.C.: Jan. 8, 2008).

research and development, and counterintelligence efforts, as well as a project to improve public/private partnerships.[20]

- *The Information Systems Security Line of Business:* The goal of this initiative, led by OMB, is to improve the level of information systems security across government agencies and reduce costs by sharing common processes and functions for managing information systems security. Several agencies have been designated as service providers for IT security awareness training and FISMA reporting.

- *Federal Desktop Core Configuration:* For this initiative, OMB directed agencies that have Windows XP deployed and plan to upgrade to Windows Vista operating systems to adopt the security configurations developed by the National Institute of Standards and Technology, Department of Defense, and Department of Homeland Security. The goal of this initiative is to improve information security and reduce overall IT operating costs.

- *SmartBUY:* This program, led by the General Services Administration, is to support enterprise-level software management through the aggregate buying of commercial software governmentwide in an effort to achieve cost savings through volume discounts. The SmartBUY initiative was expanded to include commercial off-the-shelf encryption software and to permit all federal agencies to participate in the program. The initiative is to also include licenses for information assurance.

- *Trusted Internet Connections Initiative:* This effort, directed by OMB and led by the Department of Homeland Security, is designed to optimize individual agency network services into a common solution for the federal government. The initiative is to facilitate the reduction of external connections, including Internet points of presence, to a target of 50.

We currently have ongoing work that addresses the status, planning, and implementation efforts of several of these initiatives.

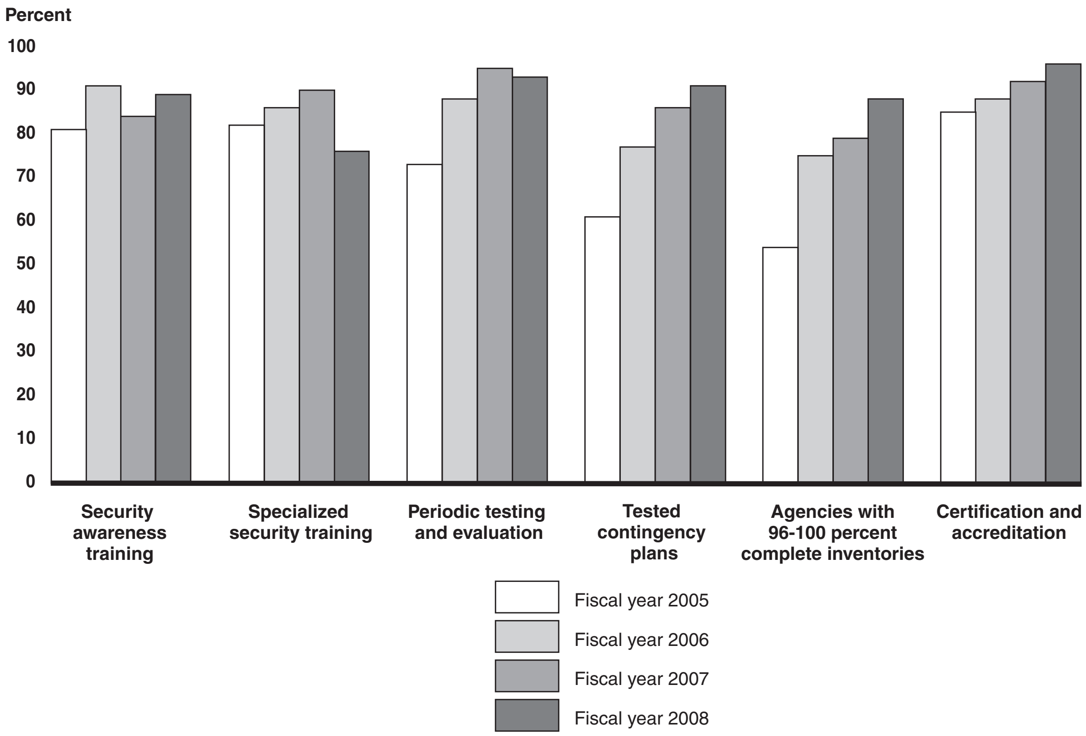
[20] Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

Agencies Continue to Report Progress in Implementing Requirements

Federal agencies reported increased compliance in implementing key information security control activities for fiscal year 2008; however, inspectors general at several agencies noted shortcomings with agencies' implementation of information security requirements. OMB also reported that agencies' were increasingly performing key activities. Specifically, agencies reported increases in the number and percentage of systems that had been certified and accredited,[21] the number and percentage of employees and contractors receiving security awareness training, and the number and percentage of systems with tested contingency plans. However, the number and percentage of systems that had been tested and evaluated at least annually decreased slightly and the number and percentage of employees who had significant security responsibilities and had received specialized training decreased significantly (see fig. 6). Consistent with previous years, inspectors general continued to identify weaknesses with the processes and practices agencies have in place to implement FISMA requirements. Although OMB took steps to clarify its reporting instructions to agencies for preparing fiscal year 2008 reports, the instructions did not request inspectors general to report on agencies' effectiveness of key activities and did not always provide clear guidance to inspectors general.

[21] Certification is a comprehensive assessment of management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision to authorize operation of an information system and to explicitly accept the risk to agency operations based on implementation of controls.

Figure 6: Reported Data for Selected Performance Metrics for 24 Major Agencies



Source: GAO analysis of IG and agency data.

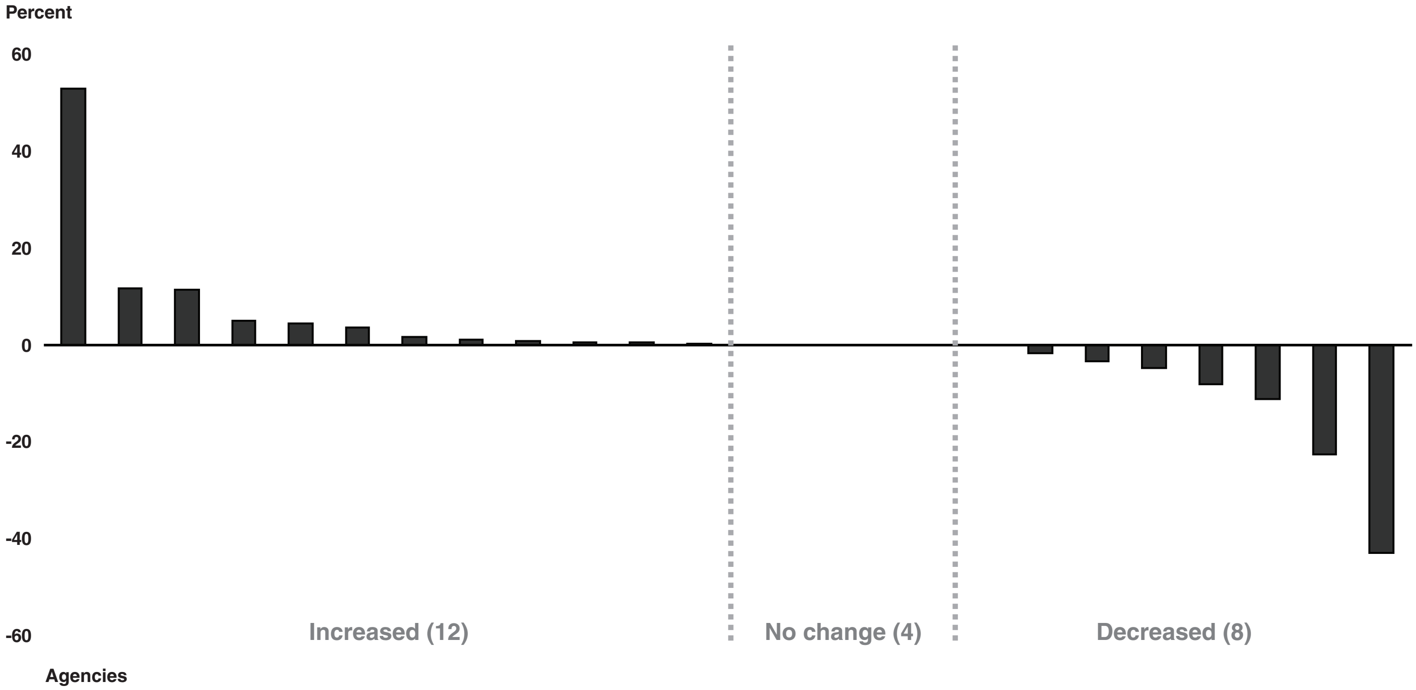
Agencies Report Mixed Progress in Implementing Security Awareness and Specialized Training

Federal agencies rely on their employees to protect the confidentiality, integrity, and availability of the information in their systems. It is critical for system users to understand their security roles and responsibilities and to be adequately trained to perform them. FISMA requires agencies to provide security awareness training to personnel, including contractors and other users of information systems that support agency operations and assets. This training should explain information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks. In addition, agencies are required to provide appropriate training on information security to personnel who have significant security responsibilities.

Agencies reported a slight increase in the percentage of employees and contractors who received security awareness training. According to agency reports, 89 percent of total employees and contractors had received security awareness training in 2008 compared to 84 percent of employees and contractors in 2007. While this change marks an improvement between fiscal years 2007 and 2008, the percentage of employees and contractors receiving security awareness training is still below the 91 percent reported for 2006. In addition, seven inspectors general reported disagreement with the percentage of employees and contractors receiving security awareness training reported by their agencies. Additionally, several inspectors general reported specific weaknesses related to security awareness training at their agencies; for example, one inspector general reported that the agency lacked the ability to document and track which system users had received awareness training, while another inspector general reported that training did not cover the recommended topics.

Governmentwide, agencies reported a lower percentage of employees who had significant security responsibilities who had received specialized training. In fiscal year 2008, 76 percent of these employees had received specialized training compared with 90 percent of these employees in fiscal year 2007. Although the governmentwide percentage decreased, the majority of the 24 agencies reported increasing or unchanging percentages of employees receiving specialized training; 8 of the 24 agencies reported percentage decreases (see fig. 7).

Figure 7: Specialized Training for 24 Major Agencies



Source: GAO analysis of agency data.

At least 12 inspectors general reported weaknesses related to specialized security training. One of the inspectors general reported that some groups did not have a training program for personnel who have critical IT responsibilities and another inspector general reported that the agency was unable to effectively track contractors who needed specialized training. Decreases in the number of individuals receiving specialized training at some federal agencies combined with continuing deficiencies in training programs could limit the ability of agencies to implement security measures effectively. Providing for the confidentiality, integrity, and availability of information in today's highly networked environment is not an easy or trivial task. The task is made that much more difficult if each person who owns, uses, relies on, or manages information and information systems does not know or is not properly trained to carry out his or her specific responsibilities.

Weaknesses Reported in Testing and Evaluating System Security Controls

Periodically evaluating the effectiveness of security policies and controls and acting to address any identified weaknesses are fundamental activities that allow an agency to manage its information security risks proactively, rather than reacting to individual problems ad hoc after a violation has been detected or an audit finding has been reported. Management control testing and evaluation as part of a program review is an additional source of information that can be considered along with controls testing and evaluation in inspector general and other independent audits to help provide a more complete picture of an agency's security posture. FISMA requires that federal agencies periodically test and evaluate the effectiveness of their information security policies, procedures, and practices as part of implementing an agencywide security program. This testing is to be performed with a frequency depending on risk, but no less than annually, and consists of testing management, and operational and technical controls for every system identified in the agency's required inventory of major information systems. For the annual FISMA reports, OMB requires that agencies identify the number of agency and contractor systems for which security controls have been tested.

In 2008, federal agencies reported testing and reviewing security controls for 93 percent of their systems, a slight decline from 95 percent in 2007. Despite this percentage remaining above 90 percent, inspectors general continued to identify deficiencies in agencies' testing and evaluation of security controls for their systems. For example, one agency's inspector general reported that systems owners only reviewed documents to assess security controls and did not use other assessment methods as suggested by NIST guidance, such as selecting samples for testing and interviewing responsible parties. Another inspector general identified instances where the agency did not document the test results in the system's security test and evaluation report. In addition, two inspectors general reported that their agencies had not always tested the controls for their systems at least annually. As a result, agencies may not have reasonable assurance that controls have been implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the security requirements of the agency.

Agencies Reported Testing More Contingency Plans, but Inspectors General often Cited Weaknesses

Continuity of operations planning ensures that agencies will be able to perform essential functions during any emergency or situation that disrupts normal operations. It is important that these plans be clearly documented, communicated to potentially affected staff, and updated to reflect current operations. In addition, testing contingency plans is essential to determining whether the plans will function as intended in an emergency situation. FISMA requires that agencywide information security programs include plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. To show the status of implementing contingency plans testing, OMB requires that agencies report the percentage of systems that have contingency plans tested in accordance with policy and guidance and requests that inspectors general also report this percentage for the subset of systems the inspector general selected for review.

Federal agencies reported that 91 percent of their systems had contingency plans that had been tested, an increase from 86 percent tested in fiscal year 2007. In addition, agencies reported progress in the number of high-risk systems with tested contingency plans; 90 percent of these systems had tested contingency plans, an increase from 77 percent in fiscal year 2007. Agencies also reported 92 percent of moderate-risk systems, 90 percent of low-risk systems, and 96 percent of uncategorized systems with tested contingency plans.

While agencies reported higher percentages of tested contingency plans, 14 inspectors general reported weaknesses in their agencies' contingency planning development and testing. For example, the inspector general of one agency reported that contingency plans were missing required elements. Regarding the testing of contingency plans, another inspector general reported that the agency had not ensured that the contractor had tested contingency plans or periodically conducted quality testing. At another agency, the inspector general reported that the agency had not performed a full, comprehensive disaster recovery test to ensure that essential and critical systems and applications could be recovered. Without developing contingency plans and ensuring that they are tested, an agency increases its risk that it will not be able to effectively recover and continue operations when an emergency occurs.

Agencies Reported More Systems, but Deficiencies Were Identified in Inventory Processes

In fiscal year 2008, 24 major agencies reported a total of 10,587 systems, composed of 8,685 agency and 1,902 contractor systems as shown by impact level in table 1. This represents a slight increase in the total number of systems from fiscal year 2007. Specifically, the number of agency systems decreased slightly and the number of contractor systems increased by 40 percent.

Table 1: Total Number of Agency and Contractor Systems in FY 2007 and FY 2008 by Impact Level

	Agency		Contractor		Total	
Impact level	FY07	FY08	FY07	FY08	FY07	FY08
High	1,089	1,043	121	113	**1,210**	**1,156**
Moderate	3,264	3,556	513	535	**3,777**	**4,091**
Low	4,351	3,943	334	738	**4,685**	**4,681**
Not categorized	229	143	384	516	**613**	**659**
Total	**8,933**	**8,685**	**1,352**	**1,902**	**10,285**	**10,587**

Source: GAO analysis of agency FY 2007 and FY 2008 FISMA reports.

Eleven inspectors general identified weaknesses in their agencies' inventory process. For example, one inspector general agreed that its agency's inventory accurately captured the number of active systems, but indicated the inventory had also included systems in development, which were not labeled as such and therefore could not be labeled and inventoried accurately. Another inspector general reported that its agency had not verified the inventory information reported by its components, but had instead relied on an honor system of reporting. Other weaknesses included contractor systems not listed in the inventory or an agency not having interfaces to other systems identified in its inventory. Without complete, accurate inventories, agencies cannot efficiently maintain and secure their systems.

Agencies Reported Higher Percentages, but Inspectors General Highlight Weaknesses in the Quality of Certifications and Accreditations

OMB has continued to emphasize its long-standing policy of requiring a management official to formally authorize (accredit) an information system to process information and accept the risk associated with its operation based on a formal evaluation (certification) of the system's security controls. For the annual FISMA reports, OMB requires agencies to identify the number of systems and impact levels authorized for processing after completing certification and accreditation. OMB requests that inspectors general also report this percentage for the subset of systems reviewed. In addition, OMB asks the inspectors general to rate the quality of the agency's certification and accreditation process on a scale of failing to excellent. Inspectors general may also indicate which aspects of the certification and accreditation process have been considered in determining that rating, such as the security plan, system impact level, system test and evaluation, security control testing, incident handling, security awareness training, configurations/patching, and other items. OMB's annual reporting template also allows the inspectors general to comment on their agencies' certification and accreditation processes.

Federal agencies reported higher percentages of systems that have been certified and accredited than in 2007. For fiscal year 2008, 96 percent of the agencies' systems were reported as being certified and accredited, as compared with 92 percent in 2007. In addition, agencies reported certifying and accrediting 98 percent of their high-risk systems, an increase from 95 percent in 2007.

Although agencies continue to report higher percentages of certified and accredited systems, inspectors general continue to report mixed results in the quality of the certification and accreditation processes at their agencies. To illustrate, 17 inspectors general reported specific weaknesses in their agency's certification and accreditation processes. For example, two inspectors general rated their agencies' certification and accreditation process as poor or failing, while both of those agencies reported that more than 90 percent of their systems had been certified and accredited. In another example, the inspector general of one agency stated that systems had been authorized to operate without sufficient testing of the adequacy of mandatory security controls. Inspectors general also cited other weaknesses, such as the security plan not providing an adequate basis for certification and accreditation and the risk assessment not identifying risks for vulnerabilities exposed by previous testing. Without ensuring the complete certification and accreditation of a system, agency officials may not have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems.

Agencies Report Having Configuration Management Policies, but Did Not Always Implement Them

Risk-based policies and procedures cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system in an information security program; a key aspect of these policies and procedures is having minimally acceptable configuration standards. Configuration standards can minimize the security risks associated with specific software applications widely used in an agency or across agencies. Because IT products are often intended for a wide variety of audiences, restrictive security controls are usually not enabled by default, making many of the products vulnerable before they are used.

FISMA requires each agency to have policies and procedures that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. In fiscal year 2008, for the first time, OMB required agencies to report on whether they had implemented security configurations prescribed under OMB's memorandum for Windows Vista and XP operating systems.[22] For annual FISMA reporting, OMB requires agencies to report whether they have an agencywide security configuration policy; the extent to which they have implemented common security configurations, including those available from the NIST Web site, on applicable systems; and whether or not they have adopted and implemented Windows XP and Vista standard configurations, documented deviations, and implemented the settings. OMB also requested inspectors general to report on their agencies' implementation of these configurations.

Reporting by agencies and inspectors general illustrates that, while many agencies had configuration policies, those policies had not always been implemented. All 24 major federal agencies reported that they had an agencywide security configuration policy. Even though 22 inspectors general agreed that their agency had such a policy, they did not agree that the implementation was always as high as the agencies had reported. For example, 12 agencies reported implementing common security configurations 96 to 100 percent of the time, but only 6 inspectors general reported this. In another example, only one agency reported implementing common security configurations 0 to 50 percent of the time, while seven inspectors general reported this level of implementation for their agencies. In addition, only seven agencies and six inspectors general reported that the agency had implemented standard security settings. If minimally acceptable configuration requirements policies are not properly implemented and applied to systems, agencies will not have assurance that products have been configured adequately to protect those systems, which could make them more vulnerable.

Most Agencies Reported Following Security Incident Procedures, but Weaknesses in Procedures Continue at Selected Agencies

Although strong controls may not block all intrusions and misuse, agencies can reduce the risks associated with such events if they take steps to detect and respond to them before significant damage occurs. Accounting for and analyzing security problems and incidents are also effective ways for an agency to improve its understanding of threats and the potential costs of security incidents, and doing so can pinpoint vulnerabilities that need to be addressed so that they are not exploited again.

[22] OMB, Memorandum M-08-22, *Guidance on the Federal Desktop Core Configuration* (Washington, D.C.: August 2008).

FISMA requires that agencies' security programs include procedures for detecting, reporting, and responding to security incidents. NIST states that agencies are responsible for determining specific ways to meet these requirements. For FISMA reporting, OMB requires agencies to state whether or not the agency follows documented policies and procedures for reporting incidents internally, to the US-Computer Emergency Readiness Team (US-CERT), and to law enforcement. OMB also requires agencies to indicate additional information about their incident detection and monitoring capabilities, including what tools and technologies the agency uses for incident detection. For FISMA reporting, inspectors general are also requested to state whether or not their agencies follow documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement.

All of the agencies reported that they had followed policies and procedures for reporting incidents internally and to law enforcement during fiscal year 2008, and only one agency reported that it had not followed documented policies and procedures for reporting incidents to US-CERT.

While the majority of inspectors general continue to report that their agencies are following documented procedures for identifying and reporting incidents internally as well as to US-CERT and to law enforcement, there was a slight increase in the number of inspectors general who reported that their agencies were not following these procedures. Six inspectors general noted that their agency was not following procedures for internal incident reporting compared to five in fiscal year 2007. Four inspectors general noted that their agency was not following reporting procedures to US-CERT compared to two in 2007, and two noted that their agency was not following reporting procedures to law enforcement compared to one in 2007.

At least 12 inspectors general also noted specific weaknesses in incident procedures such as a lack of fully documented policies and procedures for responding to security incidents, a lack of control procedures to ensure that audit trails were being maintained and reviewed, and instances where incidents were not always handled and reported in accordance with requirements. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Without proper incident response and documentation, agencies risk losing valuable information needed to prevent future exploits and to understand the nature and cost of the threats directed at them.

Agencies Report Improvements in Remedial Actions, but Processes Could Be Strengthened

Developing remedial action plans is key to ensuring that remedial actions are taken to address significant deficiencies and reduce or eliminate known vulnerabilities. These plans should list the weaknesses and show the estimated resource needs and the status of corrective actions. The plans are intended to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. FISMA requires that agency information security programs include a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices. In addition, OMB requires agencies to report quarterly regarding their remediation efforts for all programs and systems where a security weakness has been identified. It also requests that inspectors general assess and report annually on whether their agency has developed, implemented, and managed an agencywide process for these plans.

Inspectors general reported an increase in the number of agencies that had developed and implemented plans of action and milestones (POA&M) when weaknesses were identified. For 2008, 13 inspectors general reported that their agency had developed POA&Ms 96 to 100 percent of the time when weaknesses were identified; up from 11 inspectors general reporting this in 2007. However, many still cited weaknesses with their agency's POA&M process. Several mentioned that their agency did not always include weaknesses or vulnerabilities identified through security controls testing or inspector general reviews in the POA&M. They also reported that their agency did not always properly track weaknesses because the status of individual weaknesses was not always accurate. Without a sound remediation process, agencies cannot be assured that information security weaknesses have been efficiently and effectively corrected.

Inspectors General Report Using Professional Standards for Conducting Independent Evaluations More, but Opportunities to Improve Consistency Remain

An increasing number of inspectors general reported conducting annual independent evaluations in accordance with professional standards and provided additional information about the effectiveness of their agency's security programs. FISMA requires agency inspectors general or their independent external auditors to perform an independent evaluation of the information security programs and practices of the agency to determine the effectiveness of the programs and practices. We have previously reported[23] that the annual inspector general independent evaluations lacked a common approach and that the scope and methodology of the evaluations varied across agencies. We noted that there was an opportunity to improve these evaluations by conducting them in accordance with audit standards or a common approach and framework.

In fiscal year 2008, 16 of 24 inspectors general cited using professional standards to perform the annual FISMA evaluations, up from 8 inspectors general who cited using standards the previous year. Of the 16 inspectors general, 13 reported performing evaluations that were in accordance with generally accepted government auditing standards, while the other 3 indicated using the "Quality Standards for Inspections" issued by the President's Council on Integrity and Efficiency.[24] The remaining eight inspectors general cited using internally developed standards or did not indicate whether they had performed their evaluations in accordance with professional standards.

In addition, an increasing number of inspectors general provided supplemental information about their agency's information security policies and practices. To illustrate, 21 of 24 inspectors general reported additional information about the effectiveness of their agency's security controls and programs that was above and beyond what was requested in the OMB template, an increase from the 18 who had provided such additional information in their fiscal year 2007 reports. The additional information included descriptions of significant control deficiencies and

[23] GAO-07-837 and GAO, *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist*, GAO-08-571T (Washington, D.C.: Mar. 12, 2008).

[24] The President's Council on Integrity and Efficiency was established by executive order to address integrity, economy, and effectiveness issues that transcend individual government agencies and increase the professionalism and effectiveness of inspector general personnel throughout government. The Inspector General Reform Act of 2008 combined the council with the Executive Council on Integrity and Efficiency to create the Council of Inspectors General on Integrity and Efficiency.

weaknesses in security processes that provided additional context to the agency's security posture.

Although inspectors general reported using professional standards more frequently, their annual independent evaluations occasionally lacked consistency. For example,

- Three inspectors general provided only template responses and did not identify the scope and methodology of their evaluation. (These three inspectors general were also among those who had not reported performing their evaluation in accordance with professional standards.)

- Descriptions of the controls evaluated during the review as documented in the scope and methodology sections differed. For example, according to their FISMA reports, a number of inspectors general stated that their evaluations included a review of policies and procedures, whereas others did not indicate whether policies and procedures had been reviewed. Additionally, multiple inspectors general also indicated that technical vulnerability assessments had been conducted as part of the review, whereas others did not indicate whether such an assessment had been part of the review.

- Eleven inspectors general indicated that their FISMA evaluations considered the results of previous information security reviews, whereas 13 inspectors general did not indicate whether they considered other information security work, if any.

The development and use of a common framework or adherence to auditing standards could provide improved effectiveness, increased efficiency, quality control, and consistency in inspector general assessments.

Opportunities Remain for OMB to Improve Annual Reporting and Oversight of Agency Information Security Programs

Although OMB has supported several governmentwide initiatives and provided additional guidance to help improve information security at agencies, opportunities remain for it to improve its annual reporting and oversight of agency information security programs. FISMA specifies that OMB, among other responsibilities, is to develop policies, principles, standards, and guidelines on information security and report to Congress not later than March 1 of each year on agencies' implementation of FISMA. Each year, OMB provides instructions to federal agencies and their inspectors general for preparing their FISMA reports and then summarizes the information provided by the agencies and the inspectors general in its report to Congress.

Over the past 4 years, we have reported[25] that, while the periodic reporting of performance measures for FISMA requirements and related analysis provides valuable information on the status and progress of agency efforts to implement effective security management programs, shortcomings in OMB's reporting instructions limited the utility of the annual reports. Accordingly, we recommended that OMB improve reporting by clarifying reporting instructions; develop additional metrics that measure control effectiveness; request inspectors general to assess the quality of additional information security processes such as system test and evaluation, risk categorization, security awareness training, and incident reporting; and require agencies to report on additional key security activities such as patch management. Although OMB has taken some actions to enhance its reporting instructions, it has not implemented most of the recommendations, and thus further actions need to be taken to fully address them.

In addition to the previously reported shortcomings, OMB's reporting instructions for fiscal year 2008 did not sufficiently address several processes key to implementing an agencywide security program and were sometimes unclear. For example, the reporting instructions did not request inspectors general to provide information on the quality or effectiveness of agencies' processes for developing and maintaining inventories, providing specialized security training, and monitoring contractors. For these activities, inspectors general were requested to report only on the extent to which agencies had implemented the activity but not on the effectiveness of those activities. Providing information on the effectiveness of the processes used to implement the activities could further enhance the usefulness of the data for management and oversight purposes.

OMB's guidance to inspectors general for rating agencies' certification and accreditation processes was not clear. In its reporting instructions, OMB requests inspectors general to rate their agency's certification and accreditation process using the terms "excellent," "good," "satisfactory,"

[25] GAO, *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005); GAO-07-837; and GAO-08-571T.

"poor," or "failing." However, the reporting instructions do not define or identify criteria for determining the level of performance for each rating. OMB also requests inspectors general to identify the aspect(s) of the certification and accreditation process they included or considered in rating the quality of their agency's process. Examples OMB included were security plan, system impact level, system test and evaluation, security control testing, incident handling, security awareness training, and security configurations (including patch management). While this information is helpful and provides insight on the scope of the rating, inspectors general were not requested to comment on the quality or effectiveness of these items. Additionally, not all inspectors general considered the same aspects in reviewing the certification and accreditation process, yet all were allowed to provide the same rating. Without clear guidelines for rating these processes, OMB and Congress may not have a consistent basis for comparing the progress of an agency over time or against other agencies.

In its report to Congress for fiscal year 2008, OMB did not fully summarize the findings from the inspectors general independent evaluations or identify significant deficiencies in agencies' information security practices. FISMA requires OMB to provide a summary of the findings of agencies' independent evaluations and significant deficiencies in agencies' information security practices. Inspectors general often document their findings and significant information security control deficiencies in reports that support their evaluations. However, OMB did not summarize and present this information in its annual report to Congress. Most of the inspectors general information summarized in the annual report was taken from the "yes" or "no" responses or from questions having a predetermined range of percentages as stipulated by OMB's reporting template. Thus, important information about the implementation of agency information security programs and the vulnerabilities and risks associated with federal information systems was not provided to Congress in OMB's annual report. This information could be useful in determining whether agencies are effectively implementing information security policies, procedures, and practices. As a result, Congress may not be fully informed about the state of federal information security.

OMB also did not approve or disapprove agencies' information security programs. FISMA requires OMB to review agencies' information security programs at least annually and approve or disapprove them. OMB representatives informed us that they review agencies' FISMA reports and interact with agencies whenever an issue arises that requires their oversight. However, representatives stated that they do not explicitly or publicly declare that an agency's information security program has been approved or disapproved. As a result, a mechanism for establishing accountability and holding agencies accountable for implementing effective programs was not used.

Conclusions

Weaknesses in information security controls continue to threaten the confidentiality, integrity, and availability of the sensitive data maintained by federal agencies. These weaknesses, including those for access controls, configuration management, and segregation of duties, leave federal agency systems and information vulnerable to external as well as internal threats. The White House, OMB, and federal agencies have initiated actions intended to enhance information security at federal agencies. However, until agencies fully and effectively implement information security programs and address the hundreds of recommendations that we and agency inspectors general have made, federal systems will remain at an increased and unnecessary risk of attack or compromise.

Despite these weaknesses, federal agencies have continued to report progress in implementing key information security requirements. While NIST, inspectors general, and OMB have all made progress toward fulfilling their statutory requirements, the current reporting process does not produce information to accurately gauge the effectiveness of federal information security activities. OMB's annual reporting instructions did not cover key security activities and were not always clear. Finally, OMB did not include key information about findings and significant deficiencies identified by inspectors general in its governmentwide report to Congress and did not approve or disapprove agency information security programs. Shortcomings in reporting and oversight can result in insufficient information being provided to Congress and diminish its ability to monitor and assist federal agencies in improving the state of federal information security.

Recommendations for Executive Action

We recommend that the Director of the Office of Management and Budget take the following four actions:

- Update annual reporting instructions to request inspectors general to report on the effectiveness of agencies' processes for developing inventories, monitoring contractor operations, and providing specialized security training.

- Clarify and enhance reporting instructions to inspectors general for certification and accreditation evaluations by providing them with guidance on the requirements for each rating category.
- Include in OMB's report to Congress, a summary of the findings from the annual independent evaluations and significant deficiencies in information security practices.
- Approve or disapprove agency information security programs after review.

Agency Comments and Our Evaluation

In written comments on a draft of this report, the Federal Chief Information Officer (CIO)[26] generally agreed with our overall assessment of information security at the agencies. He also identified actions that OMB is taking to clarify its reporting guidance and to consider more effective security performance metrics. These actions are consistent with the intent of two of our recommendations, that OMB clarify and enhance reporting instructions and request inspectors general to report on additional measures of effectiveness.

The Federal CIO did not address our recommendation to include a summary of the findings and significant security deficiencies in its report to Congress and did not concur with GAO's conclusion that OMB does not approve or disapprove agencies' information security management programs on an annual basis. He indicated that OMB reviews all agency and IG FISMA reports annually; reviews quarterly information on the major agencies' security programs; and uses this information, and other reporting, to evaluate agencies security programs. The Federal CIO advised that concerns are communicated directly to the agencies. We acknowledge that these are important oversight activities. However, as we reported, OMB did not demonstrate that it approved or disapproved agency information security programs, as required by FISMA. Consequently, a mechanism for holding agencies accountable for implementing effective programs is not being effectively used.

[26] On March 5, 2009, the President named a Federal Chief Information Officer at the White House to direct the policy and strategic planning of federal information technology investments and be responsible for oversight of federal technology spending. The Federal CIO also establishes and oversees enterprise architecture to ensure system interoperability and information sharing and ensure information security and privacy across the federal government.

We are sending copies of this report to the Office of Management and Budget and other interested parties. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you have any questions regarding this report, please contact me at (202) 512-6244 or by e-mail at wilshuseng@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix IV.

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

In accordance with the Federal Information Security Management Act of 2002 (FISMA) requirement that the Comptroller General report periodically to Congress, our objectives were to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) federal agency implementation of FISMA requirements.

To assess the adequacy and effectiveness of agency information security policies and practices, we analyzed our related reports issued from May 2007 through April 2009. We also reviewed and analyzed the information security work and products of agency inspectors general. Further, we reviewed and summarized weaknesses identified in our reports and that of inspectors general using five major categories of information security controls: (1) access controls, (2) configuration management controls, (3) segregation of duties, (4) continuity of operations planning, and (5) agencywide information security programs. Our reports generally used the methodology contained in the *Federal Information System Controls Audit Manual*.[1] We also examined information provided by the U.S. Computer Emergency Readiness Team (US-CERT) on reported security incidents.

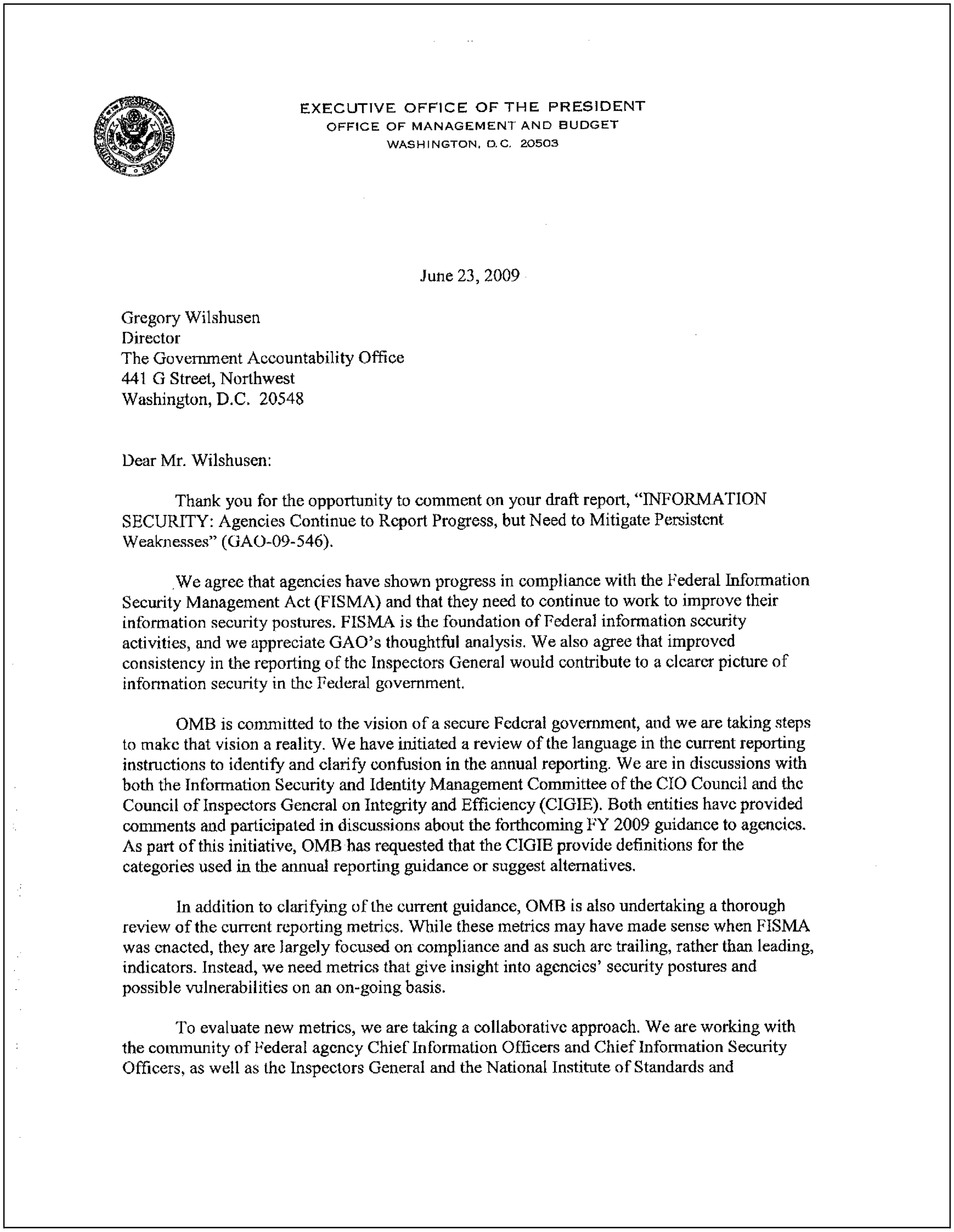
To assess the implementation of FISMA requirements, we reviewed and analyzed the provisions of the act[2] and the mandated annual FISMA reports from the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and the CIOs and IGs of 24 major federal agencies for fiscal years 2007 and 2008. We also examined OMB's FISMA reporting instructions and other OMB and NIST guidance.

We also held discussions with OMB representatives and agency officials from the National Institute of Standards and Technology and the Department of Homeland Security's US-CERT to further assess the implementation of FISMA requirements. We did not verify the accuracy of the agencies' responses; however, we reviewed supporting documentation that agencies provided to corroborate information provided in their responses. We did not include systems categorized as national security systems in our review, nor did we review the adequacy or effectiveness of the security policies and practices for those systems.

[1] GAO, *Federal Information System Controls Audit Manual*, GAO-09-232G (Washington, D.C.: February 2009).

[2] Pub. L. No. 107-347, title III, 116 Stat. 2899, 2946 (Dec. 17, 2002).

We conducted this performance audit from December 2008 to May 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 23, 2009

Gregory Wilshusen
Director
The Government Accountability Office
441 G Street, Northwest
Washington, D.C. 20548

Dear Mr. Wilshusen:

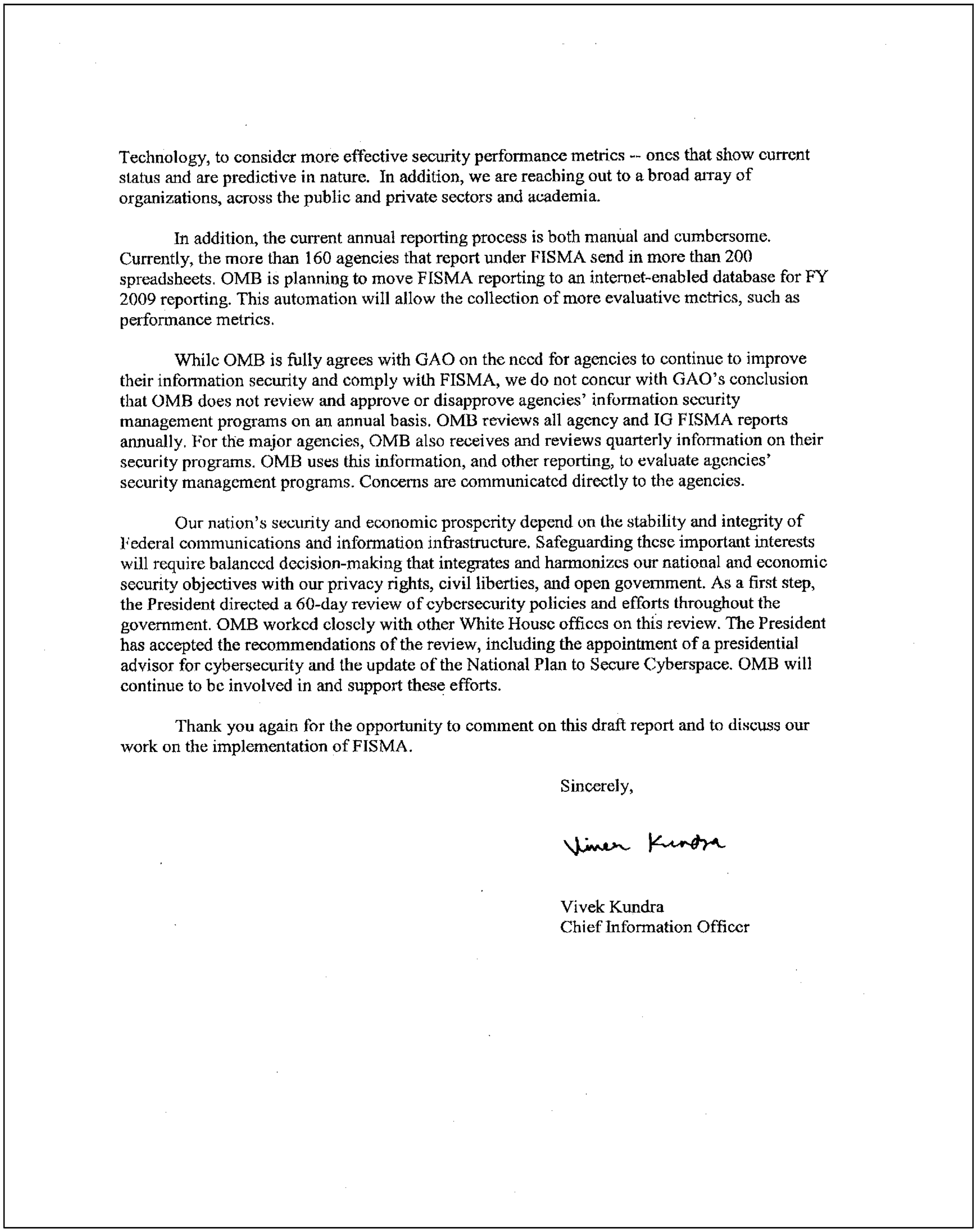
Thank you for the opportunity to comment on your draft report, "INFORMATION SECURITY: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses" (GAO-09-546).

We agree that agencies have shown progress in compliance with the Federal Information Security Management Act (FISMA) and that they need to continue to work to improve their information security postures. FISMA is the foundation of Federal information security activities, and we appreciate GAO's thoughtful analysis. We also agree that improved consistency in the reporting of the Inspectors General would contribute to a clearer picture of information security in the Federal government.

OMB is committed to the vision of a secure Federal government, and we are taking steps to make that vision a reality. We have initiated a review of the language in the current reporting instructions to identify and clarify confusion in the annual reporting. We are in discussions with both the Information Security and Identity Management Committee of the CIO Council and the Council of Inspectors General on Integrity and Efficiency (CIGIE). Both entities have provided comments and participated in discussions about the forthcoming FY 2009 guidance to agencies. As part of this initiative, OMB has requested that the CIGIE provide definitions for the categories used in the annual reporting guidance or suggest alternatives.

In addition to clarifying of the current guidance, OMB is also undertaking a thorough review of the current reporting metrics. While these metrics may have made sense when FISMA was enacted, they are largely focused on compliance and as such are trailing, rather than leading, indicators. Instead, we need metrics that give insight into agencies' security postures and possible vulnerabilities on an on-going basis.

To evaluate new metrics, we are taking a collaborative approach. We are working with the community of Federal agency Chief Information Officers and Chief Information Security Officers, as well as the Inspectors General and the National Institute of Standards and



Technology, to consider more effective security performance metrics -- ones that show current status and are predictive in nature. In addition, we are reaching out to a broad array of organizations, across the public and private sectors and academia.

In addition, the current annual reporting process is both manual and cumbersome. Currently, the more than 160 agencies that report under FISMA send in more than 200 spreadsheets. OMB is planning to move FISMA reporting to an internet-enabled database for FY 2009 reporting. This automation will allow the collection of more evaluative metrics, such as performance metrics.

While OMB is fully agrees with GAO on the need for agencies to continue to improve their information security and comply with FISMA, we do not concur with GAO's conclusion that OMB does not review and approve or disapprove agencies' information security management programs on an annual basis. OMB reviews all agency and IG FISMA reports annually. For the major agencies, OMB also receives and reviews quarterly information on their security programs. OMB uses this information, and other reporting, to evaluate agencies' security management programs. Concerns are communicated directly to the agencies.

Our nation's security and economic prosperity depend on the stability and integrity of Federal communications and information infrastructure. Safeguarding these important interests will require balanced decision-making that integrates and harmonizes our national and economic security objectives with our privacy rights, civil liberties, and open government. As a first step, the President directed a 60-day review of cybersecurity policies and efforts throughout the government. OMB worked closely with other White House offices on this review. The President has accepted the recommendations of the review, including the appointment of a presidential advisor for cybersecurity and the update of the National Plan to Secure Cyberspace. OMB will continue to be involved in and support these efforts.

Thank you again for the opportunity to comment on this draft report and to discuss our work on the implementation of FISMA.

Sincerely,

Vivek Kundra

Vivek Kundra
Chief Information Officer

In March 2009, we convened a panel of experts to discuss how to improve key aspects of the national cyber security strategy and its implementation as well as other critical aspects of the strategy, including areas for improvement. The experts, who included former federal officials, academics, and private-sector executives, highlighted 12 key improvements that are, in their view, essential to improving the strategy and our national cyber security posture. These improvements are in large part consistent with our previously mentioned reports and extensive research and experience in this area.

Table 2: Key Improvements Needed to Strengthen the Nation's Cybersecurity Posture

Cyber security improvement	Description
1. Develop a national strategy that clearly articulates strategic objectives, goals, and priorities.	The strategy should, among other things, (1) include well-defined strategic objectives, (2) provide understandable goals for the government and the private sector (end game), (3) articulate cyber priorities among the objectives, (4) provide a vision of what a secure cyber space should be in the future, (5) seek to integrate federal government capabilities, (6) establish metrics to gauge whether progress is being made against the strategy, and (7) provide an effective means for enforcing action and accountability when there are progress shortfalls. According to expert panel members, the CNCI provides a good set of tactical initiatives focused on improving primarily federal cyber security; however, it does not provide strategic objectives, goals, and priorities for the nation as a whole.
2. Establish White House responsibility and accountability for leading and overseeing national cyber security policy.	The strategy makes the Department of Homeland Security (DHS) the focal point for cyber security; however, according to expert panel members, DHS has not met expectations and has not provided the high-level leadership needed to raise cyber security to a national focus. Accordingly, panelists stated that to be successful and to send the message to the nation and cyber critical infrastructure owners that cyber security is a priority, this leadership role needs to be elevated to the White House. In addition, to be effective, the office must have, among other things, commensurate authority— for example, over budgets and resources—to implement and employ incentives that will encourage action.
3. Establish a governance structure for strategy implementation.	The strategy establishes a public/private partnership governance structure that includes 18 critical infrastructure sectors, corresponding government and sector coordinating councils, and cross-sector councils. However, according to panelists, this structure is government-centric and largely relies on personal relationships to instill trust to share information and take action. In addition, although all sectors are not of equal importance in regard to their cyber assets and functions, the structure treats all sectors and all critical cyber assets and functions equally. To ensure effective strategy implementation, experts stated that the partnership structure should include a committee of senior government representatives (for example, the Departments of Defense, Homeland Security, Justice, State, and the Treasury and the White House) and private-sector leaders representing the most critical cyber assets and functions. Expert panel members also suggested that this committee's responsibilities should include measuring and periodically reporting on progress in achieving the goals, objectives, and strategic priorities established in the national strategy and building consensus to hold involved parties accountable when there are progress shortfalls.

Cyber security improvement	Description
4. Publicize and raise awareness about the seriousness of the cyber security problem.	Although the strategy establishes cyberspace security awareness as a priority, experts stated that many national leaders in business and government, including in Congress, who can invest resources to address cyber security problems are generally not aware of the severity of the risks to national and economic security posed by the inadequacy of our nation's cyber security posture and the associated intrusions made more likely by that posture. Expert panel members suggested that an aggressive awareness campaign is needed to raise the level of knowledge of leaders and the general populace that protecting our information and systems from cyber attack is ongoing.
5. Create an accountable, operational cyber security organization.	DHS established the National Cyber Security Division (within the Office of Cybersecurity and Communications) to be responsible for leading national day-to-day cyber security efforts; however, according to panelists, this has not enabled DHS to become the national focal point as envisioned. Panel members stated that currently the Department of Defense and other organizations within the intelligence community that have significant resources and capabilities have come to dominate federal efforts. They told us that there also needs to be an independent cyber security organization that leverages and integrates the capabilities of the private sector, civilian government, law enforcement, military, intelligence community, and the nation's international allies to address incidents against the nation's critical cyber systems and functions. However, there was not a consensus among our expert panel members regarding where this organization should reside.
6. Focus more actions on prioritizing assets and functions, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.	The strategy recommends actions to identify critical cyber assets and functions, but panelists stated that efforts to identify which cyber assets and functions are most critical to the nation have been insufficient. According to panel members, inclusion in cyber critical infrastructure protection efforts and lists of critical assets are currently based on the willingness of the person or entity responsible for the asset or function to participate and not on substantiated technical evidence. In addition, the current strategy establishes vulnerability reduction as a key priority; however, according to panelists, efforts to identify and mitigate known vulnerabilities have been insufficient. They stated that greater efforts should be taken to identify and eliminate common vulnerabilities and that there are techniques available that should be used to assess vulnerabilities in the most critical, prioritized cyber assets and functions.
7. Bolster public/private partnerships through an improved value proposition and use of incentives.	While the strategy encourages action by owners and operators of critical cyber assets and functions, panel members stated that there are not adequate economic and other incentives (i.e., a value proposition) for greater investment and partnering in cyber security. Accordingly, panelists stated that the federal government should provide valued services (such as offering useful threat or analysis and warning information) or incentives (such as grants or tax reductions) to encourage action by and effective partnerships with the private sector. They also suggested that public and private sector entities use means such as cost-benefit analyses to ensure the efficient use of limited cyber security-related resources.
8. Focus greater attention on addressing the global aspects of cyberspace.	The strategy includes recommendations to address the international aspects of cyber space but, according to panelists, the United States is not addressing global issues impacting how cyber space is governed and controlled. They added that, while other nations are actively involved in developing treaties, establishing standards, and pursuing international agreements (such as on privacy), the United States is not aggressively working in a coordinated manner to ensure that international agreements are consistent with U.S. practice and that they address cyber security and cyber crime considerations. Panel members stated that the United States should pursue a more coordinated, aggressive approach so that there is a level playing field globally for U.S. corporations and enhanced cooperation among government agencies, including law enforcement. In addition, a panelist stated that the United States should work towards building consensus on a global cyber strategy.

Cyber security improvement	Description
9. Improve law enforcement efforts to address malicious activities in cyberspace.	The strategy calls for improving investigative coordination domestically and internationally and promoting a common agreement among nations on addressing cyber crime. According to one panelist, some improvements in domestic law have been made (e.g., enactment of the PROTECT Our Children Act of 2008), but implementation of this act is a work-in-process due to its recent passage. Panel members also stated that current domestic and international law enforcement efforts, including activities, procedures, methods, and laws are too outdated and outmoded to adequately address the speed, sophistication, and techniques of individuals and groups, such as criminals, terrorists, and others who have malicious intent. Improved law enforcement is essential to more effectively catch and prosecute malicious individuals and groups and, with stricter penalties, deter malicious behavior.
10. Place greater emphasis on cyber security research and development, including consideration of how to better coordinate government and private-sector efforts.	While the strategy recommends actions to develop a research and development agenda and coordinate efforts between the government and private sector, experts stated that the United States is not adequately focusing and funding research and development efforts to address cyber security or to develop the next generation of cyber space to include effective security capabilities. In addition, the research and development efforts currently under way are not being well coordinated between government and the private sector.
11. Increase the cadre of cyber security professionals.	The strategy includes efforts to increase the number and skills of cyber security professionals but, according to panelists, the results have not created sufficient numbers of professionals, including information security specialists and cyber crime investigators. Expert panel members stated that actions to increase the number of professionals with adequate cyber security skills should include (1) enhancing existing scholarship programs (e.g., Scholarship for Service) and (2) making the cyber security discipline a profession through testing and licensing.
12. Make the federal government a model for cyber security, including using its acquisition function to enhance cyber security aspects of products and services.	The strategy establishes securing the government's cyber space as a key priority and advocates using federal acquisition to accomplish this goal. Although the federal government has taken steps to improve the cyber security of agencies (e.g., beginning to implement the CNCI initiatives), panelists stated that it still is not a model for cyber security. Further, they said the federal government has not made changes in its acquisition function and the training of government officials in a manner that effectively improves the cyber security capabilities of products and services purchased and used by federal agencies.

Source: GAO.

GAO Contact

Gregory C. Wilshusen (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the individual named above, Charles Vrabel (Assistant Director); Debra Conner; Larry Crosland; Sharhonda Deloach; Neil Doherty; Kristi Dorsey; Rosanna Guererro; Nancy Glover; Rebecca Eyler; Mary Marshall; and Jayne Wilson made key contributions to this report.

Cybersecurity: Continued Federal Efforts Are Needed to Protect Critical Systems and Information. GAO-09-835T. Washington, D.C.: June 25, 2009.

Privacy and Security: Food and Drug Administration Faces Challenges in Establishing Protections for Its Postmarket Risk Analysis System. GAO-09-355. Washington, D.C.: June 1, 2009.

Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks. GAO-09-292. Washington, D.C.: May 13, 2009.

Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk. GAO-09-661T. Washington, D.C.: May 5, 2009.

Freedom of Information Act: DHS Has Taken Steps to Enhance Its Program, but Opportunities Exist to Improve Efficiency and Cost-Effectiveness. GAO-09-260. Washington, D.C.: March 20, 2009.

Information Security: Securities and Exchange Commission Needs to Consistently Implement Effective Controls. GAO-09-203. Washington, D.C.: March 16, 2009.

National Cyber Security Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture. GAO-09-432T. Washington, D.C.: March 10, 2009.

Information Security: Further Actions Needed to Address Risks to Bank Secrecy Act Data. GAO-09-195. Washington, D.C.: January 30, 2009.

Information Security: Continued Efforts Needed to Address Significant Weaknesses at IRS. GAO-09-136. Washington, D.C.: January 9, 2009.

Nuclear Security: Los Alamos National Laboratory Faces Challenges in Sustaining Physical and Cyber Security Improvements. GAO-08-1180T. Washington, D.C.: September 25, 2008.

Critical Infrastructure Protection: DHS Needs to Better Address Its Cyber Security Responsibilities. GAO-08-1157T. Washington, D.C.: September 16, 2008.

Critical Infrastructure Protection: DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise. GAO-08-825. Washington, D.C.: September 9, 2008.

Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network. GAO-08-1001. Washington, D.C.: September 9, 2008.

Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability. GAO-08-588. Washington, D.C.: July 31, 2008.

Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains. GAO-08-525. Washington, D.C.: June 27, 2008.

Information Security: FDIC Sustains Progress but Needs to Improve Configuration Management of Key Financial Systems. GAO-08-564. Washington, D.C.: May 30, 2008.

Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks. GAO-08-526. Washington, D.C.: May 21, 2008.

Information Security: TVA Needs to Enhance Security of Critical Infrastructure Control Systems and Networks. GAO-08-775T. Washington, D.C.: May 21, 2008.

Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist. GAO-08-571T. Washington, D.C.: March 12, 2008.

Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program. GAO-08-280. Washington, D.C.: February 29, 2008.

Information Security: Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies. GAO-08-496T. Washington, D.C.: February 14, 2008.

Information Security: Protecting Personally Identifiable Information. GAO-08-343. Washington, D.C.: January 25, 2008.

Information Security: IRS Needs to Address Pervasive Weaknesses. GAO-08-211. Washington, D.C.: January 8, 2008.

Veterans Affairs: Sustained Management Commitment and Oversight Are Essential to Completing Information Technology Realignment and

Strengthening Information Security. GAO-07-1264T. Washington, D.C.: September 26, 2007.

Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. GAO-07-1036. Washington, D.C.: September 10, 2007.

Information Security: Sustained Management Commitment and Oversight Are Vital to Resolving Long-standing Weaknesses at the Department of Veterans Affairs. GAO-07-1019. Washington, D.C.: September 7, 2007.

Information Security: Selected Departments Need to Address Challenges in Implementing Statutory Requirements. GAO-07-528. Washington, D.C.: August 31, 2007.

Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses. GAO-07-837. Washington, D.C.: July 27, 2007.

Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program. GAO-07-870. Washington, D.C.: July 13, 2007.

Information Security: Homeland Security Needs to Enhance Effectiveness of Its Program. GAO-07-1003T. Washington, D.C.: June 20, 2007.

Information Security: Agencies Report Progress, but Sensitive Data Remain at Risk. GAO-07-935T. Washington, D.C.: June 7, 2007.

Information Security: Federal Deposit Insurance Corporation Needs to Sustain Progress Improving Its Program. GAO-07-351. Washington, D.C.: May 18, 2007.

(311020)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper

United States Government Accountability Office

GAO

Report to Congressional Requesters

INFORMATION SECURITY

Protecting Personally Identifiable Information

GAO

Accountability ★ Integrity ★ Reliability

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-08-343, a report to congressional requesters

January 2008

INFORMATION SECURITY

Protecting Personally Identifiable Information

Why GAO Did This Study

The loss of personally identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. As shown in prior GAO reports, compromises to such information and long-standing weaknesses in federal information security raise important questions about what steps federal agencies should take to prevent them. As the federal government obtains and processes information about individuals in increasingly diverse ways, properly protecting this information and respecting the privacy rights of individuals will remain critically important.

GAO was requested to (1) identify the federal laws and guidance issued to protect personally identifiable information from unauthorized use or disclosure and (2) describe agencies' progress in developing policies and documented procedures that respond to recent guidance from the Office of Management and Budget (OMB) to protect personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter. To do so, GAO reviewed relevant laws and guidance, surveyed officials at 24 major federal agencies, and examined and analyzed agency documents, including policies, procedures, and plans. In commenting on a draft of this report, OMB stated that it generally agreed with the report's contents.

To view the full product, including the scope and methodology, click on GAO-08-343. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Two primary laws (the Privacy Act of 1974 and the E-Government Act of 2002) give federal agencies responsibilities for protecting personal information, including ensuring its security. Additionally, the Federal Information Security Management Act of 2002 (FISMA) requires agencies to develop, document, and implement agencywide programs to provide security for their information and information systems (which include personally identifiable information and the systems on which it resides). The act also requires the National Institute of Standards and Technology (NIST) to develop technical guidance in specific areas, including minimum information security requirements for information and information systems. In the wake of recent incidents of security breaches involving personal data, OMB issued guidance in 2006 and 2007 reiterating agency responsibilities under these laws and technical guidance, drawing particular attention to the requirements associated with personally identifiable information. In this guidance, OMB directed, among other things, that agencies encrypt data on mobile computers or devices and follow NIST security guidelines regarding personally identifiable information that is accessed outside an agency's physical perimeter.

Not all agencies had developed the range of policies and procedures reflecting OMB guidance on protection of personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter. Of 24 major agencies, 22 had developed policies requiring personally identifiable information to be encrypted on mobile computers and devices. Fifteen of the 24 agencies had policies to use a "time-out" function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity. Fewer agencies (11) had established policies to log computer-readable data extracts from databases holding sensitive information and erase the data within 90 days after extraction. Several agencies indicated that they were researching technical solutions to address these issues. Gaps in their policies and procedures reduced agencies' ability to protect personally identifiable information from improper disclosure.

At the conclusion of GAO's review, OMB announced in November 2007 that agencies that did not complete certain privacy and security requirements, including those just described, received a downgrade in their scores for progress in electronic government initiatives. According to OMB, it will continue working with agencies to help them strengthen their information security and privacy programs, especially as they relate to the protection of personally identifiable information. In view of OMB's recent actions in this area and GAO's previous recommendations on improving agency information security and implementation of FISMA requirements, GAO is making no further recommendations at this time.

Contents

Table

Abbreviations

FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
HIPPA	Health Insurance Portability and Accountability Act of 1996
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	privacy impact assessment
US-CERT	U.S. Computer Emergency Readiness Team
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

Washington, DC 20548

January 25, 2008

The Honorable Norm Coleman
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Susan A. Davis
House of Representatives

Concerns regarding the security of personal information on federal systems have been raised by incidents in which such information has been compromised by the loss or theft of equipment or by unauthorized access. For example, in a reported incident involving the Department of Veterans Affairs, a laptop computer containing the personal data of millions of veterans was stolen from the home of an employee in May 2006. Similar incidents have occurred at other agencies, such as an incident at the Department of Energy, detected in mid 2005, when hackers gained access to more than 1,500 records, and another in June 2006, when the Department of Agriculture reported a hacker had broken into several systems that potentially compromised personal records for up to 26,000 people.

These security breaches highlight the importance of federal agencies having effective information security controls in place to protect personally identifiable information—that is, information that can be used to locate or identify an individual, such as names, aliases, Social Security numbers, biometric records, and other personal information that is linked or linkable to an individual. Loss of such information may lead to identity theft[1] or other fraudulent use of the information, resulting in substantial harm, embarrassment, and inconvenience to individuals.

As the federal government obtains and processes information about individuals in increasingly diverse ways, it is critically important that it ensure that the privacy rights of individuals are respected and this

[1] Identity theft is the wrongful obtaining and using of another person's identifying information in some way that involves fraud or deception, typically for economic gain.

information is properly secured and protected. Security breaches that compromise such information raise important questions about the steps that federal agencies should take to prevent them.

To help answer these questions, you asked us to (1) identify the federal laws enacted and guidance issued to protect personally identifiable information from unauthorized use or disclosure and (2) describe agencies' progress in developing policies and documented procedures that respond to recent Office of Management and Budget (OMB) guidance to protect personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter.

To address the first objective, we reviewed relevant laws and guidance and determined the requirements and recommended actions relevant to securing personally identifiable information. To address the second objective, we surveyed the 24 major federal agencies and departments,[2] and we examined and analyzed agency policies, procedures, plans, and artifacts against recent OMB guidance. Appendix I contains additional details on the objectives, scope, and methodology of our review. We conducted this performance audit from September 2006 to January 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results in Brief

Two primary laws (the Privacy Act of 1974 and the E-Government Act of 2002) give federal agencies responsibilities for protecting personal information, including ensuring its security. Overall agency information security responsibilities are set forth in the Federal Information Security Management Act of 2002 (FISMA).[3] This act requires agencies to develop,

[2] The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

[3] FISMA, Title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

document, and implement agencywide programs to provide security for their information and information systems (which include personally identifiable information and the systems on which it resides). The act requires agencies, among other things, to develop risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level. In addition, to help agencies implement FISMA requirements, the act also requires the National Institute of Standards and Technology (NIST) to develop technical guidance in specific areas.[4] Accordingly, NIST has developed (1) standards for categorizing information and information systems so that agencies can provide appropriate levels of security according to risk levels (low, moderate, or high),[5] (2) guidelines recommending the types of information and information systems to be included in categories of risk,[6] and (3) minimum information security requirements for information and information systems in each category.[7] In the wake of recent incidents of security breaches involving personal data, OMB has issued guidance reiterating agency responsibilities under these laws and technical guidance, drawing particular attention to the requirements associated with personally identifiable information. In this guidance, OMB directed, among other things, that agencies encrypt data on mobile computers or devices, follow NIST security guidelines regarding personally identifiable information that is accessed outside an agency's physical perimeter, and establish core management groups to respond to security breaches involving personally identifiable information. OMB also updated and added to requirements for reporting security breaches and the loss or unauthorized access of personally identifiable information and directed agencies to develop policies for notifying those affected by such breaches.

Not all agencies had developed and documented policies and procedures reflecting OMB guidance on protection of personally identifiable information that is either accessed remotely or physically transported

[4] FISMA requires NIST to develop this guidance for systems other than national security systems.

[5] NIST, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standard (FIPS) 199 (Washington, D.C., February 2004).

[6] NIST, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*, Special Publication 800-60 (Washington, D.C., June 2004).

[7] NIST, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS 200 (Washington, D.C., March 2006).

outside an agency's secured physical perimeter. Of the 24 major agencies, 22 had developed policies requiring personally identifiable information to be encrypted on mobile computers and devices. Fifteen of the agencies had policies to use a "time-out" function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity. Fewer agencies (11) had established policies to log computer-readable data extracts for databases holding sensitive information and erase the data within 90 days after extraction. Several agencies indicated that they were researching technical solutions to address these issues. Gaps in their policies and procedures reduced agencies' ability to protect personally identifiable information from improper disclosure.

At the conclusion of our review, OMB announced that agencies that did not complete all the privacy and security requirements identified in a key OMB directive received a downgrade in their scores for E-Government progress on the President's Management Agenda Scorecard. According to OMB, it will continue working with agencies to help them strengthen their information security and privacy programs, especially as they relate to the protection of personally identifiable information. In view of OMB's recent actions in this area and our previous recommendations on improving agency information security and implementation of FISMA requirements,[8] we are making no further recommendations at this time.

In providing oral comments on a draft of this report, OMB representatives generally agreed with the report's contents.

Background

The growth in information technology, networking, and electronic storage has made it ever easier to collect and maintain information about individuals. An accompanying growth in incidents of loss and unauthorized use of such information has led to increased concerns about protecting this information on federal systems. As a result, the basic law governing privacy protections, the Privacy Act of 1974, has been supplemented by more recent laws and guidance that are particularly

[8] GAO, *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, GAO-07-837 (Washington, D.C.: July 27, 2007).

concerned with the protection of personally identifiable information maintained in automated information systems.[9]

Protecting personally identifiable information in federal systems is critical because its loss or unauthorized disclosure can lead to serious consequences for individuals. These consequences include identity theft or other fraudulent activity, which can result in substantial harm, embarrassment, and inconvenience. In 2006, the estimated losses associated with identity theft to U.S. organizations were $49.3 billion.[10]

Incidents Have Placed Personal Information at Risk

Like other sectors, the federal government has seen significant exposures of personally identifiable information. According to a 2006 congressional staff report, since January 2003, 19 departments and agencies reported at least one loss of personally identifiable information that could expose individuals to identity theft.[11] (App. II provides selected examples of these and other incidents.)

A series of data breaches at federal agencies have involved system intrusion, phishing scams,[12] and the physical loss or theft of portable computers, hard drives, and disks. During fiscal year 2006, federal agencies reported a record number of incidents to the U.S. Computer Emergency Readiness Team (US-CERT). For example, in 2006 there were 5,146 incident reports—a substantial increase over the 3,569 incidents reported in 2005. During this period, US-CERT recorded a dramatic rise in incidents where either physical loss or theft or system compromise resulted in the loss of personally identifiable information.

[9] As used in this report, the term personally identifiable information is defined as any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, biometric records, and any other personal information that is linked or linkable to an individual.

[10] GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07- 705 (Washington, D.C.: June 22, 2007).

[11] Committee on Government Reform, *Staff Report: Agency Data Breaches Since January 1, 2003* (Washington, D.C., Oct. 13, 2006).

[12] Phishing is a high-tech scam that frequently uses unsolicited messages to deceive people into disclosing their financial and/or personal identity information.

Weaknesses in Implementing Security Policies Have Persisted at Federal Agencies

As illustrated by recent security incidents and as we have previously reported,[13] significant weaknesses continued to threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. In their fiscal year 2006 financial statement audit reports, 21 of 24 major agencies indicated that deficient information security controls were either a reportable condition[14] or a material weakness.[15] Our audits continue to identify similar weaknesses in nonfinancial systems. Similarly, in their annual reporting under 31 U.S.C. § 3512 (commonly referred to as the Federal Managers' Financial Integrity Act of 1982),[16] 17 of 24 agencies reported shortcomings in information security, including 7 that considered it a material weakness. Agency inspectors general have also noted the seriousness of information security, with 21 of 24 including it as a "major management challenge" for their agencies.[17]

According to our reports and those of inspectors general, persistent weaknesses appear in the five major categories of information system controls: (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs

[13] See GAO-07-837.

[14] Reportable conditions are significant deficiencies in the design or operation of internal controls that could adversely affect the entity's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements.

[15] A material weakness is a reportable condition that precludes the entity's internal controls from providing reasonable assurance that misstatements, losses, or noncompliance material in relation to the financial statements or to stewardship information would be prevented or detected on a timely basis.

[16] FMFIA (31 U.S.C. § 3512) requires agencies to report annually to the President and Congress on the effectiveness of internal controls and any identified material weaknesses in those controls. Per OMB, for the purposes of FMFIA reporting, a material weakness also encompasses weaknesses found in program operations and compliance with applicable laws and regulations. Material weaknesses for FMFIA reporting are determined by management, whereas material weaknesses reported as part of a financial statement audit are determined by independent auditors.

[17] The Reports Consolidation Act of 2000 (31 U.S.C. § 3516(d)) requires inspectors general to include in their agencies' performance and accountability report a statement that summarizes what they consider to be the most serious management and performance challenges facing their agency and briefly assesses their agencies' progress in addressing those challenges.

are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and (5) an agencywide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented. Most agencies had weaknesses in each of these categories. Accordingly, we have designated information security as a governmentwide high-risk issue in reports to Congress since 1997—a designation that remains in force today.[18]

Federal Laws and Guidance Provide a Foundation for Agencies to Protect Personally Identifiable Information

The primary laws that provide privacy protections to personal information are the Privacy Act of 1974 and the E-Government Act of 2002; these laws describe, among other things, agency responsibilities with regard to personally identifiable information, which include providing security. The security of information held by the federal government is specifically addressed by FISMA, which requires agencies to develop, document, and implement agencywide programs to provide security for their information and information systems, including personally identifiable information. Along with technical guidance from NIST, FISMA establishes a risk-based approach to security management, which requires an agency, among other things, to categorize its information and systems according to the potential impact to the agency should the information be jeopardized. In the wake of recent incidents of security breaches involving personal data, OMB has issued guidance reiterating the requirements of these laws and guidance, drawing particular attention to those associated with personally identifiable information. In addition, OMB updated and added to requirements for reporting security breaches and the loss or unauthorized access of personally identifiable information.

[18] GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997) and GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

Privacy and Security of Personal Information Are Addressed in Several Federal Laws

The major requirements for the protection of personal privacy by federal agencies come from two laws, the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002.[19] In addition, FISMA, which is included in the E-Government Act of 2002, addresses the protection of personal information in the context of securing federal agency information and information systems.

To protect personal privacy, the Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records. The act describes a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. It also defines "system of records" as a group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public by a notice in the Federal Register identifying, among other things, the type of data collected, the types of individuals about whom information is collected, the intended "routine" uses of the data, and procedures that individuals can use to review and correct personal information.[20] The act's requirements also apply to government contractors when agencies contract for the development and maintenance of a system of records to accomplish an agency function.[21]

The provisions of the Privacy Act are consistent with and based primarily on a set of principles for protecting the privacy and security of personal

[19] No single federal law governs all uses of personally identifiable information. In addition to the laws that govern federal agency use of such information, a number of statutes provide privacy protections for information used for specific purposes or maintained by specific types of entities. For example, the Fair Credit Reporting Act applies to companies that prepare or furnish information on consumer creditworthiness, and the Video Privacy Protection Act applies to the use of video rental records.

[20] Under the Privacy Act of 1974, the term "routine use" means (with respect to the disclosure of a record) the use of such a record for a purpose that is compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7).

[21] 5 U.S.C. § 552a(m)(1).

information—the Fair Information Practices.[22] These principles have been widely adopted as the standard benchmark for evaluating the adequacy of privacy protections; one of the principles is security safeguards.[23] In this regard, the Privacy Act requires agencies to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[24]

The E-Government Act of 2002 strives to enhance protection for personal information in government information systems by requiring that agencies conduct privacy impact assessments (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. More specifically, according to OMB guidance,[25] a PIA is an analysis of how information is handled (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Agencies must conduct PIAs (1) before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form or (2) before initiating any new data collections involving personal information that will be

[22] These principles were first proposed in 1973 by a U.S. government advisory committee; they were intended to address what the committee termed a poor level of protection afforded to privacy under contemporary law. The practices include principles such as security safeguards (personally identifiable information should be protected with reasonable security safeguards), openness (the public should be kept informed about privacy policies and practices), and accountability (those controlling the collection or use of personally identifiable information should be accountable for taking steps to ensure the implementation of these principles). Congress used the committee's final report as a basis for crafting the Privacy Act of 1974. See U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (Washington, D.C., July 1973).

[23] Others include data quality, openness, individual participation, and use limitation.

[24] 5 U.S.C. § 552a(e)(10).

[25] OMB, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Sept. 26, 2003).

collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people. OMB guidance also requires agencies to conduct PIAs when a system change creates new privacy risks, for example, changing the way in which personal information is being used. The PIA requirement does not apply to all systems. For example, no assessment is required when the information collected relates to internal government operations, the information has been previously assessed under an evaluation similar to a PIA, or when privacy issues are unchanged.

Besides these primary laws, Congress has passed laws requiring protection of personally identifiable information that are agency-specific or that target a specific type of information. For example, the Veterans Benefits, Health Care, and Information Technology Act,[26] enacted in December 2006, establishes information technology security requirements for personally identifiable information that apply specifically to the Department of Veterans Affairs (VA). The act mandates, among other things, that VA develop procedures for detecting, immediately reporting, and responding to security incidents; notify Congress of any significant data breaches involving personally identifiable information; and, if necessary, provide credit protection services to those individuals whose personally identifiable information has been compromised. Another example is the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[27] which requires the Secretary of Health and Human Services to adopt standards for the electronic exchange, privacy, and security of health information. These standards apply to agencies, such as the Department of Defense and VA, to the extent they are covered by HIPAA.

FISMA is the primary law governing information security in the federal government; it also addresses the protection of personal information in the context of securing federal agency information and information systems. FISMA, which establishes a risk-based approach to security management, defines federal requirements for securing information and information systems that support federal agency operations and assets. Under the act, agencies are required to provide sufficient safeguards to cost-effectively protect their information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized restrictions on access and

[26] Pub. L. No. 109-461 (Dec. 22, 2006).

[27] Pub. L. No. 104-191 (Aug. 21, 1996).

disclosure (and thus to protect personal privacy, among other things). The act also requires each agency to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency (including those provided or managed by another agency, contractor, or other source).

Specifically, the act requires that these information security programs include, among other things,

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

In addition, FISMA requires agencies to produce an annually updated inventory of major information systems (including major national security systems) operated by the agency or that are under its control, which includes an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency.

Like protecting other information and systems, protecting personally identifiable information is dependent on agencies' having established security programs that include the elements described above. Among other things, agencies must identify the personally identifiable information in their information systems, determine the appropriate risk level associated with it, develop appropriate controls to secure it, and ensure that these controls are applied and maintained.

FISMA also establishes evaluation and reporting requirements. Under the act, each agency must have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. Evaluations of non-national security systems are to be performed by the agency inspectors general or by an independent external auditor, while evaluations related to national security systems are to be performed only by an entity designated by the agency head.

FISMA also requires each agency to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of information security policies, procedures, and practices, and compliance with the act's requirements. In addition, agency heads are required to annually report the results of their independent evaluations to OMB.[28] OMB is required to submit a report to Congress each year on agency compliance with the act's requirements, including a summary of findings of agencies' independent evaluations.

FISMA Requires NIST to Develop Security Guidance

Other major FISMA provisions require NIST to develop, for systems other than national security systems, standards for categorizing information and information systems according to risk levels, guidelines on the types of information and information systems that should be included in each category, and standards for minimum information security requirements

[28] Except that, to the extent an evaluation pertains to a national security system, only a summary and assessment of that portion of the evaluation is reported to OMB.

for information and information systems in each category. Accordingly, NIST developed the following guidance:

- Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. This standard is to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels. In addition, NIST has published Special Publication 800-60, to provide guidance on how to implement FIPS 199 and how to determine whether a system or information should be categorized as having a high-, moderate-, or low-risk impact level.

- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. This standard provides minimum information security requirements for information and information systems in each risk category.

- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. The publication provides guidelines for selecting and specifying security controls for information systems supporting the federal government.

OMB Provides Guidance Reiterating Requirements on Security and Privacy

OMB is responsible for establishing governmentwide policies and for providing guidance to agencies on how to implement the provisions of FISMA, the Privacy Act, and other federal information security and privacy laws. It has issued both recommended steps and required actions to protect federally owned information and information systems. For example, OMB memorandum M-05-08[29] directs agencies to designate a senior official with overall responsibility for information privacy issues, including taking appropriate steps to protect personally identifiable information from unauthorized use, access, disclosure, or sharing, and to protect related information systems from unauthorized access, modification, disruption, or destruction.

Following the May 2006 VA data breach, OMB issued guidance reiterating agency responsibilities under the laws and technical guidance, drawing

[29] OMB, *Designation of Senior Agency Officials for Privacy*, memorandum M-05-08 (Washington, D.C., Feb. 11, 2005).

particular attention to the requirements associated with personally identifiable information.

OMB memorandum M-06-15, *Safeguarding Personally Identifiable Information*, re-emphasizes agency responsibilities to safeguard personally identifiable information and to appropriately train employees in this regard. It also requires agencies to perform a review of their policies and procedures for the protection of personally identifiable information, including an examination of physical security, and to take corrective action.

OMB memorandum M-06-16, *Protection of Sensitive Agency Information*, asks agencies to verify that existing organizational policy adequately addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed. It recommends, among other things, that all information on mobile computers and devices be encrypted unless a written waiver is issued certifying that the computer does not contain any sensitive information. In addition, M-06-16 recommends that agencies use a NIST checklist included in the memorandum. The NIST checklist states that agencies should verify that information requiring protection as personally identifiable information is appropriately categorized as such and that it is assigned an appropriate risk impact category.

OMB also updated and added to requirements for reporting security breaches and the loss or unauthorized access of personally identifiable information. OMB memorandum M-06-19 directs agencies to report all incidents involving personally identifiable information to US-CERT within 1 hour of discovery of the incident. Further, OMB recommends that agencies establish a core management group responsible for responding to the loss of personal information in a memorandum issued September 20, 2006. In OMB memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, OMB asks agencies to identify in their yearly FISMA reports any physical or electronic incidents involving the loss of or unauthorized access to personally identifiable information. In these annual reports, agencies also are required to report numbers of incidents for the reporting period, the number of incidents the agency reported to US-CERT, and the number reported to law enforcement.

Most recently, OMB memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, requires agencies to develop and implement breach notification policies—

that is, policies governing how and under what circumstances affected parties are notified in case of a security breach. Agencies were to develop and implement such policies and associated plans within 120 days from the issuance of the memorandum (May 22, 2007).

The memorandum also reiterates four particularly important existing security requirements that agencies should already have been implementing: (1) assigning an impact level to all information and information systems, (2) implementing the minimum security requirements and controls in FIPS 200 and NIST Special Publication 800-53 respectively, (3) certifying and accrediting information systems, and (4) training employees. With regard to the first of these, OMB stressed that agencies should generally consider categorizing sensitive personally identifiable information (and information systems within which such information resides) as moderate or high impact.

In addition, this memorandum reiterates the guidance provided in memorandum M-06-16 on protection of personally identifiable information and changes earlier recommendations to requirements.

These and other OMB memorandums significant to the protection of personally identifiable information are briefly described in table 1.

Table 1: Major OMB Memorandums Related to Protection of Personally Identifiable Information

Memorandum, date	Title	Major personally identifiable information requirement or recommendation
M-05-08, Feb. 11, 2005	Designation of Senior Agency Officials for Privacy	Directs agencies to designate a senior official with overall responsibility for information privacy issues who • is accountable for ensuring agency implementation of information privacy protection; and • must take appropriate steps to protect personally identifiable information from unauthorized use, access, disclosure, or sharing, and to protect related information systems from unauthorized access, modification, disruption, or destruction.
M-06-15, May 22, 2006	Safeguarding Personally Identifiable information	Re-emphasizes agency responsibilities to safeguard personally identifiable information and to appropriately train employees in this regard. Requires agency Senior Official for Privacy to conduct a review of policies and processes, and take necessary corrective actions to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information.

Memorandum, date	Title	Major personally identifiable information requirement or recommendation
M-06-16, June 23, 2006	Protection of Sensitive Agency Information	Recommends that all agencies • encrypt all data on mobile computers/devices that carry agency data unless the data are determined to be nonsensitive; • allow remote access only with two-factor authentication, where one factor is provided by a device separate from the computer gaining access; • use a “time-out” function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity; and • log all computer-readable data extracts from databases holding sensitive information and verify that each extract including sensitive data has been erased within 90 days. Recommends that agencies use a NIST security checklist, included in the memo, that provides specific actions to be taken by agencies to protect personally identifiable information that is either accessed remotely or physically transported outside an agency’s secured physical perimeter.
M-06-19, July 12, 2006	Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments	Requires agencies to report all incidents involving personally identifiable information to US-CERT within 1 hour of discovering the incident (this revises previous guidelines for reporting security incidents).
M-06-20, July 17, 2006	FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management	Requires agencies to identify in their yearly FISMA reports any physical or electronic incidents involving the loss of or unauthorized access to personally identifiable information.
M-07-16, May 22, 2007	Safeguarding Against and Responding to the Breach of Personally Identifiable Information	Requires agencies to develop and implement a breach notification policy and plan, including policy for the notification of the public, and provides the elements that must be included in the policies, including the incident reporting requirements of M-06-19. Restates recommendations of M-06-16 as requirements. Requires agencies to establish an agency response team to ensure adequate coverage and implementation of the plan. Requires agencies to review and reduce the volume of personally identifiable information to the minimum necessary and reduce the use of Social Security numbers. Updates incident reporting and handling requirements. Requires agencies’ breach notification policy and plan to lay out employees’ roles and responsibilities for handling breaches of personally identifiable information, as well as relationships with contractors or partners.

Source: GAO analysis of OMB memorandums.

Not All Agencies Had Developed Policies and Procedures Reflecting OMB Guidance on Protection of Personally Identifiable Information

Ensuring that agency policies and procedures appropriately emphasize the protection of personally identifiable information in accordance with applicable laws and guidance is an important aspect of protecting personal privacy. In recent guidance, OMB directed agencies to encrypt and otherwise protect personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter.[30] Specifically, agencies were required to

- encrypt[31] all data on mobile computers or devices that carry agency data, unless the data are determined to be nonsensitive;
- allow remote access only with two-factor authentication, where one of the factors is provided by a device separate from the computer gaining access;
- use a "time-out" function for remote access and mobile devices that requires that users re-authenticate after 30 minutes of inactivity; and
- log all instances in which computer-readable data are extracted from databases holding sensitive information, and verify that each extract including sensitive data has been erased within 90 days or that its use is still required.

OMB also recommended the use of a NIST-provided checklist for the protection of remote information, which was included in memorandum M-06-16. The checklist provides specific actions to be taken by federal agencies for the protection of personally identifiable information that is categorized as moderate or high impact and that is either accessed remotely or physically transported outside an agency's secured, physical perimeter, including information transported on removable media and on portable or mobile devices such as laptop computers and personal digital assistants. The controls and assessment methods and procedures in the checklist are a subset of what is currently required under NIST Special Publications 800-53 and 800-53A for moderate- and high-impact information systems. In addition, NIST standard (FIPS 140-2, *Security Requirements for Cryptographic Modules*) is to be used by federal

[30] OMB memorandum M-06-16, *Protection of Sensitive Agency Information*, presented this guidance as recommendations. OMB memorandum M-07-16 established the recommendations as requirements.

[31] Encryption is a method of providing basic data confidentiality and integrity by transforming plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm.

organizations when it is specified that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data. All encryption modules that protect sensitive data must follow this standard.

However, not all agencies had developed policies and procedures reflecting OMB guidance for protecting personally identifiable information that is accessed remotely or physically transported outside an agency's secured perimeter. Of the 24 major agencies, 22 had developed policies requiring personally identifiable information to be encrypted on mobile computers and devices. A smaller number of agencies had policies to provide other protections recommended by OMB, 14 of the agencies had two-factor authentication policies for remote access. Fifteen of the agencies had policies to use a "time-out" function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity. One agency used a reauthentication time shorter than 30 minutes (15 minutes). Fewer agencies (11) had established policies to log computer-readable data extracts from databases holding sensitive information and erase the data within 90 days after extraction. However, several of the agencies that had not established such policies indicated that they were researching technical solutions to address these issues.

Four agencies had policies requiring the use of the NIST checklist recommended by OMB. In addition, 20 agencies had written policies that require encryption software to be NIST FIPS 140-2 compliant.[32]

Gaps in their policies and procedures reduce agencies' ability to protect personally identifiable information from improper disclosure. The loss of personally identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. Because agencies maintain significant amounts of information concerning individuals, agencies should be more vigilant to protect that information from loss and misuse.

At the conclusion of our review and with the recent release of OMB's President's Management Agenda Scorecard for the fourth quarter of fiscal year 2007, OMB announced that agencies that did not complete all the

[32] NIST, *Security Requirements for Cryptographic Modules*, FIPS 140-2 (Washington, D.C., May 2001).

privacy and security requirements identified in OMB memorandum M-07-16, which included the requirements just described, received a downgrade in their scores for E-Government progress. According to OMB, it will continue working with agencies to help them strengthen their information security and privacy programs, especially as they relate to the protection of personally identifiable information. In view of OMB's recent actions in this area, we are making no recommendations at this time.

We reiterate, however, as we have in the past, that although having specific policies and procedures in place is an important factor in helping agencies to secure their information systems and to protect personally identifiable information, proper implementation of these policies and procedures remains crucial. Agencies' implementation of OMB's guidance on personally identifiable information, as well as our previous recommendations on improving agency information security and implementation of FISMA requirements,[33] will be essential in improving the protection of personally identifiable information.

Agency Comments

In providing oral comments on a draft of this report, OMB representatives stated that they generally agreed with the report's contents. In addition, they provided technical comments that we incorporated into the report.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to interested congressional committees and other interested parties. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at www.gao.gov.

[33] See GAO-07-837. This report noted that almost all of the 24 major federal agencies had weaknesses in one or more areas of information security controls, including preventing, limiting, or detecting access to computer networks, systems, or information.

If you have questions about this report, please contact me at (202) 512-6244. I can also be reached by e-mail at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Our objectives were to (1) identify the federal laws and guidance issued to protect personally identifiable information from unauthorized use or disclosure and (2) describe agencies' policies and documented procedures that respond to recent Office of Management and Budget (OMB) guidance to protect personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter.

To address our first objective, we identified and reviewed legislative requirements for the protection of personally identifiable information by federal agencies. Specifically, we reviewed

- the Privacy Act of 1974;
- the E-Government Act of 2002;
- the Federal Information Security Management Act of 2002;
- the Veterans Benefits, Health Care, and Information Technology Act of 2006; and
- the Health Insurance Portability and Accountability Act of 1996.

We also reviewed policy and guidance issued by OMB[1] and National Institute of Standards and Technology (NIST) relevant to agencies' policies and procedures to safeguard personally identifiable information.

To address our second objective, we selected 24 major agencies and assessed the status of their policies and procedures addressing recent OMB guidance addressing personally identifiable information.[2] At our request, each agency completed a survey of personally identifiable information practices and provided related policies and procedures. The survey and document request were based on requirements and

[1] See table 1 for a description of relevant OMB memorandums.

[2] The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

recommendations in the OMB guidance. We examined survey responses and compared agency-documented policies and procedures to OMB's requirements and guidance for consistency and sufficiency. We did not evaluate the effectiveness of agencies' implementation of the practices. However, we reviewed applicable prior GAO and agency inspector general reports and discussed whether agency policies had been fully implemented with applicable agency information technology officials.

We conducted this performance audit from September 2006 to January 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The incidents noted here were reported by government agencies between November 2004 and January 2007. Many of these incidents included the loss of personally identifiable information. These incidents were selected to provide illustrative examples of the types of incidents that occurred during this period.

- November 3, 2004, Department of Education: information of 8,290 individuals lost in the mail

  A contractor to the Federal Student Aid program sent the personal information of 8,290 individuals via a commercial shipping company. After determining that the package had been lost in transit, the department decided not to notify the affected individuals. It discontinued using that carrier for that facility as a result.

- November 24, 2004, Department of Veterans Affairs (VA): personal information accidentally disclosed on public drive of VA e-mail system

  A public drive on a VA e-mail system permitted entry by all users to folders and files containing personally identifiable information (name, Social Security number, date of birth, and in some cases personal health information such as surgery schedules, diagnosis, status, etc.) of veterans after computer system changes were made. All folders were then restricted and the individual services were contacted to limit user access.

- December 6, 2004, Department of Veterans Affairs: two personal computers stolen, exposing data of 2,000 research subjects

  Two desktop personal computers were stolen from a locked office in the research office of a medical center. One of the computers had files containing names, Social Security numbers, next of kin, addresses, and phone numbers of approximately 2,000 research subjects. The computers were password protected by the standard VA password system. The medical center immediately contacted the agency privacy officer for guidance. Letters were mailed to all research subjects informing them of the computer theft and potential for identity theft. VA enclosed letters addressed to three major credit agencies and postage paid envelopes. This incident was reported to VA and federal incident offices.

- December 17, 2004, Department of Agriculture: e-mail sent out to 1,537 individuals whose personally identifiable information was potentially exposed

An e-mail was sent to 1,537 people that included an attachment with the Social Security numbers and other personal information of all 1,537 individuals. In response to the event, a letter of apology was sent and training on appropriate security measures was developed.

- February 24, 2005, Department of Agriculture: hacker obtains access

  A system containing research data was breached when someone cracking a password or a user account installed hacking software. The agency reports that no data were compromised but that the hacker had read and write access to the server and opened access points.

- March 4, 2005, Department of Veterans Affairs: list of Social Security numbers of 897 providers inadvertently sent via e-mail

  An employee reported e-mailing a list of the names and Social Security numbers of 897 providers to a new transcription company. This was immediately reported and a supervisor called the transcription company and spoke with the owner and requested that the company destroy the file immediately. Notification letters were sent out to all 897 providers. Disciplinary action was taken against the employee.

- June 17, 2005, Department of Defense: potential unauthorized access found

  A systems administrator discovered potential unauthorized access to the Air Force Personnel Center Assignment Management System with personally identifiable information on 33,000 military members. Notifications were sent out to system users and an investigation was begun.

- Mid 2005, Department of Energy: a hacker accessed more than 1,500 records

  In June 2006, it was announced a hacker had gained access to a file containing the names and Social Security numbers of 1,502 individuals. This event, which was detected in mid 2005, was not reported to senior Department officials until June 2006.

- October 14, 2005, Department of Veterans Affairs: personal computer stolen, exposing data on 421 patients

A personal computer was stolen from a medical center that contained information on 421 patients and included patient names, last four digits of their Social Security number, height, weight, allergies, medications, recent lab results, and diagnoses. The agency's privacy officer and medical center information security officer were notified. The use of credit monitoring was investigated and it was determined that, because the entire Social Security number was not listed, it would not be necessary to use these services at the time.

- November 5, 2005, Department of Education: personally identifiable information of 11,329 student borrowers lost

  The unencrypted magnetic tape was lost from the Federal Student Aid's Virtual Data Center. After an investigation, no criminal activity was found and the case was closed.

- November 18, 2005, Department of Health and Human Services: contractor employees steal records of approximately 1,574

  Two employees of the Centers for Medicare & Medicaid Services contractor stole records for the purpose of identity theft. The approximately 1,574 individuals were notified.

- February 15, 2006, Department of Health and Human Services: 22 laptops stolen from contractor site, exposing information on 1,382

  The Centers for Disease Control and Prevention reported 22 laptops stolen from a contractor's facility; 3 of them contained Department of Defense service member information affecting 1,382 personnel. All of the potentially impacted individuals were notified.

- March 17, 2006, Department of Defense: thumb drive with personally identifiable information of approximately 207,570 Marines lost

  The information on approximately 207,570 enlisted Marines from 2001 to 2005 was lost. A notification letter was sent to the affected individuals and the Marine Corps.

- March 28, 2006, Department of Health and Human Services: eight laptops stolen from contractor, exposing information on 10,855

Eight laptops containing beneficiary and supplier information were stolen from the contractor's office. The beneficiary list on the laptops included 10,855 names, addresses, and dates of birth.

- April 5, 2006, Department of Defense: hackers access Tricare Management Activity, exposing personal data

  Hackers accessed a system containing personally identifiable information on military employees. Approximately 14,000 active duty and retired service members and dependents were affected and notified. New security measures were implemented.

- April 11, 2006, Department of Veterans Affairs: hacker and employee compromise systems, exposing information on 79,000 veterans

  A former VA employee was suspected of hacking into a medical center computer system with the assistance of a current employee who provided rotating administrator passwords. All systems in the medical center serving 79,000 veterans were compromised.

- May 3, 2006, Department of Veterans Affairs: computer equipment containing personally identifiable information of approximately 26.5 million veterans and active duty members of the military was stolen

  Computer equipment containing personally identifiable information on approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee.

- June 3, 2006, Department of Agriculture: systems compromised and potentially exposed information on 26,000

  Three Department of Agriculture computers system were compromised, potentially exposing the personally identifiable information of 26,000 individuals, including photographs. The department notified the individuals.

- June 19, 2006, Department of Education: package with personally identifiable information of 13,700 study respondents lost

  The shipping contractor to the department's National Center for Education Statistics lost a package containing the personally identifiable information of 13,700 study respondents.

- June 22, 2006, Department of Health and Human Services: laptop stolen from contractor employee, exposing information on 49,572

  The theft of a contractor employee's laptop containing a variety of personally identifiable information including medical information was reported. A total of 49,572 Medicare beneficiaries may have been affected. All were notified.

- July 1, 2006, Department of Commerce: documents and database copied by a former employee, exposing 934 employees

  A former employee copied sensitive letters and a database of employee information. The database included information on 883 cases and the letters had medical information on 51 employees.

- July 27, 2006, Department of Transportation: laptop stolen from car of DOT Inspector General, exposing information on approximately 133,000

  A laptop containing personally identifiable information of approximately 133,000 Florida pilots, commercial drivers, and other Florida residents was stolen from a government-owned vehicle.

- August 1, 2006, Department of Defense: laptop falls off motorcycle, losing personally identifiable information of 30,000

  A laptop containing personally identifiable information on 30,000 applicants, recruiters, and prospects fell off a motorcycle belonging to a Navy recruiter.

- August 3, 2006, Department of Veterans Affairs: desktop computer stolen, exposing financial records of approximately 18,000 patients

  A desktop computer was stolen from a secured area at a contractor's facility in Virginia that processes financial accounts for VA. The desktop computer was not encrypted. Notification letters were mailed and credit monitoring services offered.

- September 6, 2006, Department of Veterans Affairs: laptop stolen, exposing patient information on an unknown number of individuals

  A laptop attached to a medical device was stolen. The information on an unknown number of individuals was exposed. Notification letters and credit protection services were offered to 1,575 patients.

- January 22, 2007, Department of Veterans Affairs: external hard drive missing or stolen, exposing records on 535,000 veterans and 1.3 million non-VA physician provider records

  An external hard drive was discovered missing or stolen, exposing records on 535,000 veterans and 1.3 million non-VA physician provider records from a research facility in Birmingham, Alabama. Notification letters were sent to veterans and providers, and credit monitoring services were offered to those individuals whose records contained personally identifiable information.

GAO Contact

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the individual named above, Shaun Byrnes, Barbara Collier, Susan Czachor, Kristi Dorsey, Nancy Glover, Joshua Hammerstein, Anthony Molet, David Plocher, Charles Vrabel (Assistant Director), and Jeffrey Woodward were key contributors to this report.

(310582)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, jarmong@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

PRINTED ON RECYCLED PAPER

United States Government Accountability Office

GAO

Report to Congressional Requesters

PERSONAL INFORMATION

Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown

G A O

Accountability * Integrity * Reliability

June 2007

PERSONAL INFORMATION

Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-737, a report to congressional requesters

Why GAO Did This Study

In recent years, many entities in the private, public, and government sectors have reported the loss or theft of sensitive personal information. These breaches have raised concerns in part because they can result in identity theft—either account fraud (such as misuse of credit card numbers) or unauthorized creation of new accounts (such as opening a credit card in someone else's name). Many states have enacted laws requiring entities that experience breaches to notify affected individuals, and Congress is considering legislation that would establish a national breach notification requirement.

GAO was asked to examine (1) the incidence and circumstances of breaches of sensitive personal information; (2) the extent to which such breaches have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements. To address these objectives, GAO reviewed available reports on data breaches, analyzed 24 large data breaches, and gathered information from federal and state government agencies, researchers, consumer advocates, and others.

What GAO Recommends

This report contains no recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-737.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David G. Wood at (202) 512-8678 or woodd@gao.gov.

What GAO Found

While comprehensive data do not exist, available evidence suggests that breaches of sensitive personal information have occurred frequently and under widely varying circumstances. For example, more than 570 data breaches were reported in the news media from January 2005 through December 2006, according to lists maintained by private groups that track reports of breaches. These incidents varied significantly in size and occurred across a wide range of entities, including federal, state, and local government agencies; retailers; financial institutions; colleges and universities; and medical facilities.

The extent to which data breaches have resulted in identity theft is not well known, largely because of the difficulty of determining the source of the data used to commit identity theft. However, available data and interviews with researchers, law enforcement officials, and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft, particularly the unauthorized creation of new accounts. For example, in reviewing the 24 largest breaches reported in the media from January 2000 through June 2005, GAO found that 3 included evidence of resulting fraud on existing accounts and 1 included evidence of unauthorized creation of new accounts. For 18 of the breaches, no clear evidence had been uncovered linking them to identity theft; and for the remaining 2, there was not sufficient information to make a determination.

Requiring affected consumers to be notified of a data breach may encourage better security practices and help mitigate potential harm, but it also presents certain costs and challenges. Notification requirements can create incentives for entities to improve data security practices to minimize legal liability or avoid public relations risks that may result from a publicized breach. Also, consumers alerted to a breach can take measures to prevent or mitigate identity theft, such as monitoring their credit card statements and credit reports. At the same time, breach notification requirements have associated costs, such as expenses to develop incident response plans and identify and notify affected individuals. Further, an expansive requirement could result in notification of breaches that present little or no risk, perhaps leading consumers to disregard notices altogether. Federal banking regulators and the President's Identity Theft Task Force have advocated a notification standard—the conditions requiring notification—that is risk based, allowing individuals to take appropriate measures where the risk of harm exists, while ensuring they are only notified in cases where the level of risk warrants such action. Should Congress choose to enact a federal notification requirement, use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications of breaches that present little risk.

Contents

Table

Figure

Abbreviations

DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FTC	Federal Trade Commission
SSN	Social Security number
USPIS	United States Postal Inspection Service
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

Washington, DC 20548

June 4, 2007

The Honorable Spencer Bachus
Ranking Member
Committee on Financial Services
House of Representatives

The Honorable Michael N. Castle
House of Representatives

The Honorable Darlene Hooley
House of Representatives

The Honorable Steven C. LaTourette
House of Representatives

The Honorable Dennis Moore
House of Representatives

As a result of advances in computer technology and electronic storage, many different sectors and entities now maintain electronic records containing vast amounts of personal information on virtually all American consumers. In recent years, a number of entities—including financial service firms, retailers, universities, and government agencies—have collectively reported the loss or theft of large amounts of sensitive personal information. Some of these data breaches—such as those involving TJX Companies and the Department of Veterans Affairs (VA)—have received considerable publicity and have highlighted concerns about the protections afforded sensitive personal information.[1] Policymakers, consumer advocates, and others have raised concerns that data breaches can contribute to identity theft, in which an individual's sensitive personal

[1] In January 2007, The TJX Companies, Inc., publicly disclosed a data breach that compromised sensitive personal information, including credit and debit card data, associated with more than 45 million customer accounts. In May 2006, VA reported that computer equipment containing sensitive personal information on approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee. The equipment was eventually recovered, and forensic analysts concluded that it was unlikely that the personal information contained therein was compromised. See GAO, *Privacy: Lessons Learned About Data Breach Notification*, GAO-07-657 (Washington, D.C.: Apr. 30, 2007).

information is used fraudulently. The Federal Trade Commission (FTC), which is responsible for taking complaints from victims and sharing them with law enforcement agencies, has noted that identity theft is a serious problem—millions of Americans are affected each year, and victims may face substantial costs and time to repair the damage to their good name and credit record.

Although there is no commonly agreed-upon definition, the term “data breach” generally refers to an organization’s unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers.[2] Data breaches can take many forms and do not necessarily lead to identity theft. The term “identity theft” is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else’s name. Depending on the type of information compromised and how it is misused, identity theft victims can face a range of potential harm, from the inconvenience of having a credit card reissued to substantial financial losses and damaged credit ratings.

Beginning with California in 2002, at least 36 states have enacted breach notification laws—that is, laws that require certain entities that experience a data breach to notify individuals whose personal information was lost or stolen. There is no federal statute that requires most companies or other entities to notify affected individuals of data breaches, although federal banking regulatory agencies have issued guidance on breach notification

[2] In this report we use “personally identifiable information” to refer to any information that can be used to distinguish or trace an individual’s identity—such as name, Social Security number, driver’s license number, and mother’s maiden name—because such information generally may be used to establish new accounts, but not to refer to other “means of identification,” as defined in 18 U.S.C. § 1028(7), including account information such as credit or debit card numbers.

to the banks, thrifts, and credit unions they supervise.[3] In addition, the Office of Management and Budget has issued guidance—developed by the President's Identity Theft Task Force—on responding to data breaches at federal agencies.[4] Because a number of bills have been introduced in Congress that would establish a national breach notification requirement, you asked us to review the costs and benefits of such a requirement and the link between data breaches and identity theft.[5] As agreed with your offices, this report examines (1) what is known about the incidence and circumstances of breaches of sensitive personal information; (2) what information exists on the extent to which breaches of sensitive personal information have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements.

This report focuses on breaches of sensitive personal data that can be used to commit identity theft, and not on breaches of other sensitive data, such as medical records or proprietary business information. To address the first two objectives, we obtained and analyzed information on data breaches that have been reported in the media and aggregated by three

[3] *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (Mar. 29, 2005). The five federal banking regulatory agencies are the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the National Credit Union Administration. The National Credit Union Administration issued its guidance (which was substantially identical) separately from the other four regulators (*see* Security Program and Appendix B—Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, 70 Fed. Reg. 22764 (May 2, 2005)).

[4] The President's Identity Theft Task Force—chaired by the Attorney General and cochaired by the Chairman of the Federal Trade Commission and comprising 17 federal agencies and departments—was charged with developing a comprehensive national strategy to combat identity theft. Exec. Order No. 13,402, *Strengthening Federal Efforts to Protect Against Identity Theft*, 71 Fed. Reg. 27945 (May 10, 2006). The task force's guidance was distributed in a memorandum from the Office of Management and Budget to the heads of federal agencies and departments. *See* Office of Management and Budget Memorandum for the Heads of Departments and Agencies, *Recommendations for Identity Theft Related Data Breach Notification*, Sept. 20, 2006. In May 2007, the Office of Management and Budget issued a memorandum that updated the September 2006 guidance and, among other things, required agencies to develop and implement breach notification policies within 120 days. *See* Office of Management and Budget Memorandum for the Heads of Executive Departments and Agencies, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, M-07-16 (May 22, 2007).

[5] *See*, for example, Data Security Act of 2007, H.R. 1685, 110th Cong. (2007); Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007); Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007); Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007); and Identity Theft Prevention Act, S. 1178, 110th Cong. (2007).

private research and advocacy organizations, as well as information on breaches collected by state agencies in New York and North Carolina, federal banking regulators, and federal law enforcement agencies.[6] We also collected information on breaches experienced by federal agencies compiled by the House Government Reform Committee in 2006 and by the Department of Homeland Security (DHS).[7] In addition, we conducted a literature search of relevant articles, reports, and studies. We also conducted interviews with, and obtained documents from, representatives of federal agencies, including the FTC, the Department of Justice, DHS, and the federal banking regulatory agencies; selected state government agencies and the National Association of Attorneys General; private and nonprofit research organizations; and consumer protection and privacy advocacy groups. Further, we obtained information from industry and trade associations representing key sectors—including financial services, retail sales, higher education, health care, and information services—that have experienced data breaches. In addition, for the second objective, we examined the 24 largest (in terms of number of records breached) data breaches reported by the news media from January 2000 through June 2005 and tracked by private groups. For each of these breaches, we reviewed media reports and other publicly available information, and conducted interviews, where possible, with representatives of the entities that experienced the breaches, in an attempt to identify any known instances of identity theft that resulted from the breaches. We also examined five breaches that involved federal agencies, which were selected because they represented a variety of different circumstances. For the third objective, we reviewed the federal banking regulatory agencies' proposed and final guidance related to breach notification, and interviewed representatives of each agency regarding their consideration of potential costs, benefits, and challenges during development of the guidance. Further, we reviewed the strategic plan and other documents issued by the President's Identity Theft Task Force. In addition, we conducted a review of the effects of California's breach notification law, which included interviewing and gathering information from California

[6] The three private organizations are Attrition, Identity Theft Resource Center, and Privacy Rights Clearinghouse. We reviewed data on breaches in New York and North Carolina because they represent two large states that maintain centralized information on data breaches.

[7] The House Government Reform Committee was renamed the House Oversight and Government Reform Committee in the 110th Congress.

state officials and selected California companies, educational institutions, and other entities subject to the law's notification requirements.

We conducted our review from August 2006 through April 2007 in accordance with generally accepted government auditing standards. A more extensive discussion of our scope and methodology appears in appendix I.

Results in Brief

While comprehensive data do not exist, available evidence suggests that breaches of sensitive personal information have occurred frequently and under widely varying circumstances. For example, more than 570 data breaches have been reported in the news media from January 2005 through December 2006, according to our analysis of lists maintained by three private organizations that track such breaches. Further, a House Government Reform Committee survey of federal agencies identified more than 788 data breaches at 17 agencies from January 2003 through July 2006. Of the roughly 17,000 federally supervised banks, thrifts, and credit unions, several hundred have reported data breaches to their federal regulators over the past 2 years. In addition, officials in New York State—which requires public and private entities to report data breaches to a centralized source—reported receiving notice of 225 breaches from December 7, 2005, through October 5, 2006. Data breaches have occurred across a wide range of entities, including federal, state, and local government agencies; retailers; financial institutions; colleges and universities; and medical facilities. Some studies indicate that most publicly reported breaches resulted from intentional actions, such as a stolen laptop computer, rather than accidental occurrences, such as a lost laptop computer, but this may be because breaches related to criminal activity are perhaps more likely to be reported. Media-reported breaches have varied significantly in size, ranging from 10 records to tens of millions of records. Most of these breaches have compromised data that included personally identifiable information, while others have involved only account information such as credit card numbers.

The extent to which data breaches result in identity theft is not well known, in large part because it can be difficult to determine the source of the data used to commit identity theft. Although we identified several cases where breaches reportedly have resulted in identity theft—that is, account fraud or unauthorized creation of new accounts—available data and interviews with researchers, law enforcement officials, and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft. For example, our review of the 24 largest breaches that appeared in the news media from January 2000 through June 2005 found that 3 breaches appeared to have resulted in fraud on existing accounts, and 1 breach appeared to have resulted in the unauthorized creation of new accounts. For 18 of the breaches, no clear evidence had been uncovered linking them to identity theft; and for the remaining 2, we did not have sufficient information to make a determination. Determining the link between data breaches and identity theft is challenging, primarily because identity theft victims often do not know how their personal information was obtained, and it may be up to a year or more before stolen data are used to commit a crime. Some studies by private researchers have found little linkage between data breaches and identity theft, although our review found these studies had methodological limitations. Finally, the circumstances of a breach can greatly affect the potential harm that can result. For example, unauthorized creation of new accounts generally can occur only when a breach includes personally identifiable information. Further, breaches that are the result of intentional acts generally are considered to pose more risk than accidental breaches, according to federal officials.

Requiring consumer notification of data breaches may encourage better data security practices and help deter or mitigate harm from identity theft, but it also involves monetary costs and challenges such as determining an appropriate notification standard. Representatives of federal banking regulators, other government agencies, industry associations, and other affected parties told us that breach notification requirements have encouraged companies and other entities to improve their data security practices to minimize legal liability or avoid public relations risks that may result from a publicized breach of customer data. Further, notifying affected consumers of a breach gives them the opportunity to mitigate potential risk—for example, by reviewing their credit card statements and credit reports, or placing a fraud alert on their credit files. Some privacy advocates and others have noted that even when the risk of actual financial harm is low, breach notification is still important because individuals have a basic right to know how their personal information is being handled and when it has been compromised. At the same time, affected entities incur monetary costs to comply with notification requirements. For example, 31 companies that responded to a 2006 survey said they incurred an average of $1.4 million per breach, for costs such as mailing notification letters, call center expenses, courtesy discounts or services, and legal fees. In addition, organizations subject to notification requirements told us they face several challenges, including the lack of clarity in some state statutes about when a notification is required, difficulty identifying and locating affected individuals, and difficulty complying with varying state requirements. Notification standards—that is, the circumstances surrounding a data breach that "trigger" the required notification—vary among the states. Some parties, such as the National Association of Attorneys General, have advocated that a breach notification requirement should apply broadly in order to give consumers a greater level of protection and because the risk of harm is not always known. The guidance provided by federal banking regulators lays out a more risk-based approach, aimed at ensuring that affected individuals receive notices only when they are at risk of identity theft or other related harm. Such an approach was also adopted by the President's Identity Theft Task Force, which recommended a risk-based standard for breach notification applicable to both government agencies and private entities. As we have noted in the past, care is needed in defining appropriate criteria for incidents that merit notification. Should Congress choose to enact a federal breach notification requirement, use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications of breaches that present little risk.

This report contains no recommendations. We provided a draft of this report to FTC and provided selected portions of the draft to federal banking regulatory agencies and relevant federal law enforcement agencies. These agencies provided technical comments, which we have incorporated in this report as appropriate.

Background

Breaches of sensitive personal data in recent years at companies, universities, government agencies, and other organizations have heightened public awareness about data security and the risks of identity theft, and have led to the introduction of breach notification requirements in many state legislatures. As of April 2007, at least 36 states had enacted some form of law requiring that affected individuals be notified in the event of a data breach; California's law, enacted in 2002, was the first such state requirement.[8] States' notification requirements vary, particularly with regard to the applicable notification standard—the event or circumstance that triggers a required notification. Requirements also vary in terms of the data to which they apply—for example, some apply to paper documents as well as electronic records.

[8] Cal. Civ. Code § 1798.82.

There is currently no federal statute that requires most companies and other entities that experience a data breach to notify individuals whose personal information was lost or stolen. However, the Gramm-Leach-Bliley Act established requirements for federally supervised financial institutions to safeguard customer information.[9] To clarify these requirements, the federal banking regulators issued interagency guidance in 2005 to the banks, thrifts, and credit unions they supervise related to their handling of data breaches. Under this guidance, these institutions are expected to develop and implement a response program to address unauthorized access to customer information maintained by the institution or its service providers; and if they experience a breach, they are to notify their primary federal regulator as soon as possible and—depending on the circumstances of the incident—notify their affected customers. In addition, in September 2006 the President's Identity Theft Task Force developed guidance for federal agencies on responding to breaches involving agency data, including the factors to consider in determining whether to notify affected individuals. The task force released a strategic plan for combating identity theft in April 2007, which contained among its recommendations a proposal for establishing a national breach notification requirement.[10] Further, in December 2006, the Department of Veterans Affairs Information Security Enhancement Act of 2006 became law, which, among other things, requires VA to prescribe regulations providing for the notification of data breaches occurring at the department.[11] A number of bills have been introduced in Congress that would more broadly require companies and other entities to notify

[9] Pub. L. No. 106-102, tit. V, subtit. A, 113 Stat. 1338 (Nov. 12, 1999) (*codified at* 15 U.S.C. § 6801-6809).

[10] President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* (Washington, D.C.: Apr. 11, 2007).

[11] Pub. L. No. 109-461, tit. IX, 120 Stat. 3450 (Dec. 22, 2006), *codified at* 38 U.S.C. § 5721-5728, 7901-7907.

individuals when such breaches occur, and Congress has held several hearings related to data breaches.[12]

Identity theft occurs when individuals' identifying information is used without authorization in an attempt to commit fraud or other crimes.[13] There are two primary forms of identity theft. First, identity thieves can use financial account identifiers, such as credit card or bank account numbers, to take over an individual's existing accounts to make unauthorized charges or withdraw money. Second, thieves can use identifying data, which can include such things as SSNs and driver's license numbers, to open new financial accounts and incur charges and credit in an individual's name, without that person's knowledge. This second form of identity theft is potentially the most damaging because, among other things, it can take some time before a victim becomes aware of the problem, and it can cause substantial harm to the victim's credit rating. While some identity theft victims can resolve their problems quickly, others face substantial costs and inconvenience repairing damage to their credit records. According to FTC, millions of Americans have their identities stolen each year. Roughly 85 percent of these cases involve the misuse of existing accounts and 35 percent involve new account creation or other fraud. (Twenty percent of the total involve both.) Identity thieves obtain sensitive personal information using a variety of methods. One potential source is a breach at an organization that maintains large amounts of sensitive personal information. However, identity theft can also occur as a result of the loss or theft of data maintained by an individual, such as a lost or stolen wallet or a thief digging through household trash.

[12] For example, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before the Senate Comm. on Banking, Housing, and Urban Affairs*, 109th Cong., 1st Sess. (2005); *Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use: Hearing Before the Senate Comm. on the Judiciary*, 109th Cong., 1st Sess. (2005); *Assessing Data Security: Preventing Breaches and Protecting Sensitive Information: Hearing Before the House Comm. on Financial Services*, 109th Cong., 1st Sess. (2005); *Securing Consumers' Data: Options Following Security Breaches: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection of the House Comm. on Energy and Commerce*, 109th Cong., 1st Sess. (2005).

[13] For additional information on identity theft, see GAO, *Identity Theft: Some Outreach Efforts to Promote Awareness of New Consumer Rights Are Under Way*, GAO-05-710 (Washington, D.C.: Jun. 30, 2005) and *Identity Theft: Prevalence and Cost Appear to be Growing*, GAO-02-363 (Washington, D.C.: Mar. 1, 2002).

The Identity Theft and Assumption Deterrence Act of 1998 made identity theft a federal crime and charged FTC with taking complaints from identity theft victims; sharing these complaints with federal, state, and local law enforcement agencies; and providing the victims with informational materials to assist them.[14] Because identity theft is typically not a stand-alone crime but rather a component of one or more crimes such as bank fraud, credit card fraud, and mail fraud, a number of federal law enforcement agencies can have a role in investigating identity theft crimes, including the Federal Bureau of Investigation (FBI), U.S. Postal Inspection Service (USPIS), U.S. Secret Service (Secret Service), the Office of the Inspector General of the Social Security Administration, and Immigration and Customs Enforcement.

Available Evidence Indicates That Data Breaches Occur Frequently and Under Varying Circumstances

Available evidence from media reports, federal and state agencies, and private institutions, collectively, suggests that data breaches occur with some frequency. For example, our analysis of the lists of data breaches compiled by three private research and advocacy organizations shows more than 570 breaches reported by the news media from January 2005 through December 2006. Data breaches have occurred across a range of entities, including federal, state, and local government agencies; retailers; financial institutions; colleges and universities; and medical facilities. Breaches have varied in size and have resulted from both criminal actions and accidental incidents. Most of the breaches reported in the news media have involved data that included personal identifiers such as SSNs, while others have involved only account information such as credit card numbers.

Several Sources Indicate That Breaches of Sensitive Personal Information Are Frequent

No federal agency or other organization tracks all data breaches, and definitions of what constitutes a data breach may vary. Although there are no comprehensive data on the extent of data breaches nationwide, government officials, trade association representatives, researchers, and consumer and privacy advocates we interviewed agreed that breaches of sensitive personal information occur frequently. For example, representatives of a variety of organizations—including the Department of

[14] Pub. L. No. 105-318, 112 Stat. 3007 (Oct. 30, 1998). In addition to FTC, other federal agencies maintain data on identity theft. For example, the Internet Crime Complaint Center, a joint venture of the FBI and the National White Collar Crime Center, receives Internet-related identity theft complaints, which it shares with law enforcement agencies throughout the country.

Justice, California's Office of Privacy Protection, the Consumer Data Industry Association (a trade group representing many information resellers), and the Ponemon Institute (a private research organization)—characterized data breaches in the United States as being "prevalent" or "common." Although we did not identify comprehensive data on the extent of data breaches, available information from several sources does corroborate the anecdotal evidence that such breaches occur frequently.[15]

Media Reports

Over the past few years, several hundred data breaches have been reported each year by newspapers and other news media. Three private organizations that focus on information privacy and security issues—Privacy Rights Clearinghouse, Identity Theft Resource Center, and Attrition—track data breaches reported in newspapers, magazines, and other publicly available sources of news and information.[16] Our analysis of the three lists of data breaches maintained by these organizations indicated that at least 572 breaches were reported in the news media from January 2005 through December 2006.[17] These breaches were reported to

[15] Because the breaches cited in this section of the report derive from different sources, there may be some overlap among the numbers cited by these sources.

[16] Privacy Rights Clearinghouse is a nonprofit consumer education and advocacy project whose purpose is to advocate for consumers' privacy rights in public policy proceedings. Identity Theft Resource Center is a nonprofit organization that provides consumer and victim support and advises governmental agencies, legislators, and companies on the issue of identity theft. Attrition is an information security-related Web site maintained by volunteers.

[17] Representatives of these three organizations indicated that their definition of a data breach was consistent with the definition used in this report. However, we did not independently confirm whether the individual breaches reported by the media and tracked by these groups met the criteria for this definition, and it is possible that some of them do not. We reviewed these lists as they appeared as of February 15, 2007; additional breaches that occurred during the 2-year period we reviewed may have been subsequently added as they were discovered. Our analysis eliminated overlap among the three lists; the 572 breaches we cite represent unique breaches that appeared on at least one list.

have affected more than 80 million records.[18] However, for several reasons, these lists likely understate the true extent of data breaches in the United States. First, organizations might not voluntarily disclose data breaches that they experience. Second, some breaches that organizations do disclose may not appear in the news media, particularly if the breach was limited in scope. Finally, the three organizations compiling these lists may not have identified all of the breaches reported in the news media—for example, many breaches did not appear on all three lists, suggesting that none represents an exhaustive list of all breaches that have appeared in the news.

Federal Law Enforcement Agencies

Officials at federal law enforcement agencies told us that each year they conduct a significant number of criminal investigations that involve alleged breaches of sensitive personal information. For example, officials of the FBI's Cyber Division told us that presently it has more than 1,300 pending cases of computer or network intrusions where data breaches resulted from unauthorized electronic access to computer systems, such as hackings, at public and private organizations.[19] Officials at the Secret Service, which investigates certain cases where financial information has been lost or stolen, told us that in 2006, the service opened 327 cases involving network intrusions or other breaches at retailers, banks, credit card processors, telephone companies, educational institutions, and other organizations. Officials noted that they have seen a steady increase in the number of data breaches since 1986, when they began tracking computer fraud violations. Investigators at USPIS, the division of the U.S. Postal

[18] There were 83 million records collectively reported to have been affected by the 572 breaches. However, in some cases, the number of records affected was unknown or unreported, and the total does not reflect those breaches. Also, the number of breached records containing personal information may not be the same as the number of individuals affected by breaches because some individuals may be victims of more than one breach or may have multiple records compromised in a single breach. Finally, in addition to the 83 million records, as many as 40 million additional records may have been affected by a single breach involving the credit card processor CardSystems, although the exact number of affected records is unclear. In a complaint following the breach, FTC alleged that a hacker obtained unauthorized access to magnetic stripe data for tens of millions of credit and debit cards. However, according to testimony by a CardSystems official, only 263,000 of these records (containing 239,000 discrete account numbers) included sensitive personal information.

[19] According to these officials, not all 1,300 pending computer intrusion cases necessarily involved breaches that compromised sensitive personal information, although the vast majority have. The term hacking is commonly used to refer to accessing a computer system without authorization, with the intention of destroying, disrupting, or carrying out illegal activities on the network or computer system.

Service that investigates mail fraud, external mail theft, fraudulent changes of addresses, and other postal-related crimes, told us that the agency does not specifically track the number of data breaches in the private sector. However, despite limited data, investigators said their impression is that such data breaches likely occur frequently.

House Government Reform Committee and DHS

To obtain information on the prevalence of data breaches at federal agencies, in July 2006 the House Government Reform Committee asked federal agencies to provide details about incidents involving the loss or compromise of any sensitive personal information held by an agency or contractor from January 1, 2003, through July 10, 2006. Our analysis of the committee's report found that 17 agencies reported that they experienced at least one breach and, collectively, the agencies reported to the committee more than 788 separate incidents.[20]

The Federal Information Security Management Act of 2002 requires all federal agencies to report computer security incidents to a federal incident response center.[21] The U.S. Computer Emergency Readiness Team—a component of DHS that monitors computer security incidents at federal agencies—serves as this response center. As such, data breaches at federal agencies involving certain sensitive information must be reported to the

[20] Government Reform Committee, U.S. House of Representatives, *Staff Report: Agency Data Breaches Since January 1, 2003* (Washington, D.C.: Oct. 13, 2006). The federal agencies covered in the report were the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, and Veterans Affairs, as well as the Office of Personnel Management and the Social Security Administration. In addition to 788 incidents reported by 16 federal agencies, the Committee received information on data breaches from the Department of Veterans Affairs, which the report characterized only as "hundreds" of incidents.

[21] Pub. L. No. 107-347, tit. III, 116 Stat. 2946 (Dec. 17, 2002), *codified at* 44 U.S.C. § 3541-3549; 40 U.S.C. § 11331.

team within 1 hour of discovery of the incident.[22] DHS staff told us that they receive information about breaches at federal agencies on a daily basis. In fiscal year 2006, the center tracked 477 incidents at 59 federal agencies or at federal contractors with access to government-owned data, according to information available as of January 29, 2007. In addition, a March 2007 audit investigation found that at least 490 laptop computers owned by the Internal Revenue Service and containing taxpayer information had been lost or stolen since 2003.[23]

Federal Banking Regulators

The 2005 guidance issued by the five federal banking regulators provided that a depository institution should notify its primary federal regulator when it becomes aware of an incident involving unauthorized access to or use of sensitive customer information.[24] The guidance applies to breaches that have occurred at the financial institutions themselves, as well as third-party entities such as data processors that act as service providers and maintain customer information.[25] The five regulators differ in their methods and criteria for tracking breaches, but collectively they have tracked several hundred breaches over the past few years at roughly

[22] Office of Management and Budget Memorandum for Chief Information Officers, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, M-06-19 (July 12, 2006). The U.S. Computer Emergency Readiness Team defines a computer security incident as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practice" and the Office of Management and Budget requires reporting if the incident includes personally identifiable information, which under its definition refers to "any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual."

[23] Treasury Inspector General for Tax Administration, *The Internal Revenue Service Is Not Adequately Protecting Taxpayer Data on Laptop Computers and Other Portable Electronic Media Devices*, Ref. No. 2007-20-048 (Washington, D.C.: Mar. 23, 2007).

[24] 70 Fed. Reg. 15736 (Mar. 29, 2005) and 70 Fed. Reg. 22764 (May 2, 2005).

[25] Only data breaches at the financial institutions and at third-party entities that are their service providers and maintain their customer information are subject to the guidance; this requirement is codified at 12 C.F.R. Pt. 30, App. B, Supp. A § II(A)(2); 12 C.F.R. Pt. 208, App. D-2, Supp. A § II(A)(2); 12 C.F.R. Pt. 225, App. F, Supp. A § II(A)(2); 12 C.F.R. Pt. 364, App. B, Supp. A § II(A)(2); 12 C.F.R. Pt. 570, App. B, Supp. A § II(A)(2); and 12 C.F.R. Pt. 748, App. B § II(A)(2). However, data collected by the regulators may also include some breaches that affected their institutions but were not covered by the guidance.

17,000 institutions they supervise and at third-party entities.[26] For example, the Federal Deposit Insurance Corporation (FDIC)—the primary federal supervisor for more than 5,000 state-chartered banks that are not members of the Federal Reserve System—received reports of 194 breaches at its regulated institutions from May 2005 through December 2006, as well as reports of 14 breaches at third-party companies that also affected these institutions' customers. Similarly, officials at the Office of Thrift Supervision—which supervises more than 860 savings associations—told us that from April 2005 through December 2006, 56 of its institutions reported breaches at the institution itself and approximately 72 reported breaches at third-party entities that maintained their customer information.

State Agencies

Some states require entities experiencing data breaches to report them to designated state agencies.[27] For example, the New York State Information Security Breach and Notification Act requires entities that experience security breaches to notify the state Attorney General's Office, Consumer Protection Board, and the state Office of Cyber Security and Critical Infrastructure Coordination in cases when New York residents must be notified.[28] Such data breaches include the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of unencrypted private information. Officials of the Office of New York State Attorney General told us that from December 7, 2005, through October 5, 2006, their office received notice of 225 breaches. Similarly, a North Carolina law requires that breaches of personal information (maintained in computerized, paper, or other media) affecting at least 1,000 persons be reported to the Consumer Protection Division of the state Office of the Attorney General.[29] An official in that office told us that from December 2005 through December 2006, it had received reports of 91 breach incidents.

[26] Regulators note that while they track breaches occurring at third-party service providers involving customer information of regulated financial institutions, these breaches are typically due to lapses in data security by the third-party entity and not the financial institution itself.

[27] We did not determine the precise number of states with centralized reporting requirements. For illustrative purposes, we obtained information on data breaches from New York and North Carolina because they are two large states known to require that data breaches be reported to state agencies.

[28] N.Y. Gen. Bus. Law § 899-aa.

[29] N.C. Gen. Stat § 75-65.

Other Sources

Information that we obtained from several other sources suggests that breaches of sensitive personal information occur with some frequency across a variety of sectors. For example,

- EDUCAUSE, a nonprofit association that addresses technology issues in higher education, conducted a survey in 2005 on data security at higher education institutions in the United States and Canada. Twenty-six percent of the 490 institutions that responded said they had experienced a security incident in the past year that resulted in the compromise of confidential information.[30]

- The American Hospital Association collected information, at our request, in October 2006 from a nonrepresentative group of 46 large hospitals on breaches of sensitive personal information (excluding medical records) that they had experienced since January 2003. Collectively, 13 of the 46 hospitals reported a total of 17 data breach incidents.[31]

- The Ponemon Institute, a private company that researches privacy and security practices, conducted a survey of 51,433 U.S. adults and received responses from 9,154 (a response rate of about 18 percent). About 12 percent of the survey respondents said they recalled receiving notification of a data security breach involving their personal information.[32]

- The CMO Council, an organization serving marketing executives, reported that 16 percent of consumers who responded to a Web-based panel reported that a company had lost or compromised their personal,

[30] EDUCAUSE Center for Applied Research, *Safeguarding the Tower: IT Security in Higher Education 2006*, Volume 6, 2006.

[31] The association received information from 46 of the 78 hospitals it surveyed, a response rate of 59 percent. As agreed in advance, to preserve confidentiality the association provided us with a summary of their findings but did not identify the hospitals, and we did not independently verify the data.

[32] Ponemon Institute, LLC, *National Survey on Data Security Breach Notification* (Sept. 26, 2005). The reliability of this study's findings may be limited by a low survey response rate.

financial, or medical information. An additional 32 percent of respondents said they were not sure.[33]

- Several other studies, while not focusing specifically on breaches of sensitive personal information, have found more generally that information security vulnerabilities are widespread among U.S. and global companies.[34]

Information from multiple sources indicates that data breaches at companies, government agencies, retailers, and other entities have occurred frequently in recent years, involving millions of records of sensitive personal information. We have reported in the past that no federal law explicitly requires most companies and other entities to safeguard all of the sensitive personal information they may hold. We also have suggested that to ensure that sensitive personal information is protected on a more consistent basis, Congress should consider expanding requirements to safeguard such information.[35] The frequency of data breaches identified in this report underscores the need for entities in the public and private sectors to improve the security of sensitive personal information and further corroborates that additional federal action may be needed in this area.

Source, Cause, Size, and Content of Breaches Have Varied Widely

According to government officials, researchers, and media reports, data breaches have occurred among a wide variety of entities and as a result of both intentional actions and accidental losses. These breaches also have varied in size and in the types of data compromised.

Type of Entity

Data breaches have been reported at a wide range of public and private institutions, including federal, state, and local government agencies; public

[33] CMO Council, *Securing the Trust of Your Brand: How Security and IT Integrity Influence Corporate Reputation*, September 2006. The reliability of this study's findings may be limited because they are based on a self-selected group of respondents to a Web-based panel. Also, we were unable to determine a response rate because, according to a CMO Council representative, the total number of survey respondents was not available.

[34] For example, see Deloitte, *2006 Global Security Survey* (2006); Small Business Technology Institute, *Small Business Information Security Readiness* (San Jose, California: July 2005); Ponemon Institute, LLC, *U.S. Survey: Confidential Data at Risk* (Aug. 15, 2006); and Ponemon Institute, LLC, *Benchmark Study of European and U.S. Corporate Privacy Practices* (Apr. 26, 2006).

[35] GAO, *Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data*, GAO-06-674 (Washington, D.C.: Jun. 26, 2006).

and private colleges and universities; hospitals and other medical facilities; retailers; banks and other financial institutions; information resellers; and others. For example, in the weeks leading up to the highly publicized 2005 CardSystems breach, the media also had reported breaches at, among other entities, a large hospital, a university, a global financial institution, a federal regulatory agency, and a major technology company.

According to Attrition, of the breaches it tracked as reported in the news media in 2005 and 2006, 33 percent of the breaches occurred at educational institutions, 32 percent at financial services institutions, 25 percent at government agencies, and 10 percent at medical facilities, although breaches reported in the news media may not be representative of all breaches.[36] Similarly, the data security firm ID Analytics examined 70 data breaches that were reported by the news media from February through September 2005. According to company officials, 46 percent of these breaches occurred at educational institutions, 16 percent at financial institutions, 14 percent at retailers, 11 percent at government agencies, 7 percent at medical facilities, and 6 percent at information resellers.[37]

Another way to analyze where data breaches have occurred is to look at the number of *records* breached (as opposed to the number of breaches themselves). Our analysis of the list maintained by Attrition found that 54 percent of breached records involved financial institutions, 34 percent involved government agencies, 4 percent involved educational institutions, and 3 percent involved medical facilities. ID Analytics' report found that 57 percent of breached records involved financial institutions, 22 percent involved retailers, 13 percent involved educational institutions, 4 percent involved information resellers, 2 percent involved government agencies, and 2 percent involved medical facilities.

Cause of Breach

According to government officials, researchers, and media reports, data breaches of sensitive personal information have occurred as a result of both intentional actions as well as negligence or accidental losses. In some cases, individuals intentionally steal information for the purpose of

[36] For our analysis, we used the categories provided by Attrition for the industry sector where the breach occurred. We did not independently verify the accuracy of these categorizations.

[37] ID Analytics, Inc., *National Data Breach Analysis* (San Diego, California: January 2006). The data we cite reflect a combination of data presented in the report and additional data provided to us by ID Analytics.

committing fraud or identity theft. Breaches involving intentional actions have included:

- *Hacking*, or accessing computer systems without authorization. For example, in 2007 the retailer TJX Companies reported unauthorized intrusions into its computer systems that may have breached millions of customers' credit card and driver's license information.

- *Employee theft*. For example, in 2006, a former employee of the American Red Cross pled guilty to stealing personally identifiable information from a blood donor database.

- *Theft of physical equipment*. In 2005, for instance, a laptop containing the names and SSNs of more than 98,000 students, alumni, and others was stolen from the University of California at Berkeley.

- *Deception or misrepresentation to obtain unauthorized data*. In 2005, the information reseller ChoicePoint acknowledged that the personal records it held on approximately 162,000 consumers had been compromised by individuals who posed as legitimate subscribers to the company's information services.

Breaches involving negligence or accidental losses of data have included the following:

- *Loss of laptop computers or other hardware*. For example, in 2006, the Department of Labor reported that an employee lost a laptop containing personal information on 1,137 individuals.

- *Loss of data tapes*. For example, in 2004, Bank of America lost backup tapes containing personal information of 1.2 million government charge card holders while the tapes were being transported to a data center.

- *Unintentional exposure on the Internet*. In 2006, according to media reports, the U.S. Department of Education left unprotected on a Web site the personally identifiable information, including SSNs, of up to 21,000 recipients of federal student loans.

- *Improper disposal of data*, such as leaving sensitive personal data on unshredded documents in a publicly accessible dumpster.

We did not identify comprehensive data that reliably provide overall statistics on the causes of known data breaches. However, our review of the 24 largest data breaches reported in the news media (discussed in more detail later in this report) found that 12 breaches apparently involved intentional acts by hackers or employees illegally accessing or using data, 5 involved stolen laptops or other computer equipment, 4 involved lost computer backup tapes, 2 involved the use of deception to gain access to data, and 1 involved the possible unauthorized disclosure of data. In addition, some studies indicate that most breaches reported in the news media resulted from intentional acts rather than accidental occurrences such as a lost laptop computer. For example, in its study of 70 breaches, ID Analytics determined that 48 involved thefts committed with the apparent intention of accessing sensitive data. Eleven of the breaches involved thefts where sensitive consumer information was apparently stolen inadvertently as part of another crime (such as the theft of a laptop computer for its resale value), and another 11 breaches involved accidental loss (such as misplacement of a laptop computer). However, these data may overrepresent the proportion of all breaches that involve criminal activity, as such breaches are probably more likely than accidental losses to be reported to authorities and by the news media.

Number of Records Breached

Our analysis of the list maintained by Attrition of breaches reported by the news media found the median number of records breached to be 8,650. However, these data breaches varied considerably in size—ranging, for example, from a breach involving 10 records at a law firm to a breach involving as many as tens of millions of records at a credit card processing company. The breaches involving federal agencies that were reported to the House Government Reform Committee also varied in size—for example, several affected fewer than five records, while a breach at VA affected 26.5 million records.

Types of Data Breached

Comprehensive information does not exist on the types of data involved in all known data breaches. Among the list maintained by Attrition of breaches reported by the news media in 2005 and 2006—which may not be representative of all breaches—more than half involved SSNs and 11 percent involved credit card numbers (and 3 percent of the total involved both). In the remaining breaches, other types of account or personal information were involved, or the type of data breached was not reported. Logically, there may be an association between the type of data compromised and the type of entity experiencing the breach. For example, several educational institutions have experienced breaches of SSNs, which they may maintain as student identifiers, and several retail stores have experienced breaches of credit card numbers, which they often maintain on their customers.

Consequences of Data Breaches Are Not Fully Known, but Clear Evidence of Identity Theft Has Been Found in Relatively Few Breaches

Comprehensive information on the outcomes of data breaches is not available. Several cases have been identified in which a data breach appears to have resulted in identity theft, but available data and information from law enforcement and industry association representatives indicated that most breaches have not resulted in detected incidents of identity theft. For example, of 24 very large breaches we reviewed, 3 appeared to have resulted in fraud on existing accounts and 1 in the unauthorized creation of new accounts. Determining the link between data breaches and identity theft is challenging because, among other things, identity theft victims often do not know how their personal information was obtained. However, the circumstances of a breach, including the type of information compromised and how the breach occurred, can greatly affect the potential risk of identity theft.

Federal Law Enforcement Agencies and Industry Associations Identified Limited Instances of Breaches Leading to Identity Theft

In general, representatives of law enforcement agencies, industry and trade associations, and consumer and privacy advocacy organizations told us that no comprehensive data are available on the consequences of data breaches. Several cases have been identified where there is evidence that a data breach resulted in identity theft, including account fraud or unauthorized creation of new accounts. At the same time, available data and information from the officials we contacted indicated that most breaches have not resulted in detected incidents of identity theft.

We asked representatives of the FBI, Secret Service, USPIS, and Immigration and Customs Enforcement—a component of DHS that has investigated cases where stolen identities were used to secure jobs—the extent to which data breaches they investigated resulted in some form of identity theft. Representatives of all of these agencies told us that their investigations of data breaches do not typically allow them to fully ascertain how stolen data are used. Similarly, they noted that investigations of identity theft do not always reveal the source of the data used to commit the crime.

However, the representatives were able to provide us with a limited number of examples in which data breaches they investigated had allegedly resulted in some form of identity theft. For example, in a 2006 investigation by USPIS, an employee of a credit card call center allegedly compromised at least 35 customers' accounts and used some of the information to purchase approximately $65,000 in gift cards. The representatives of federal law enforcement agencies noted that cases in which data breaches have been linked to identity theft often have involved instances of unauthorized access by employees. For example, an official at

Immigration and Customs Enforcement stated that her agency, in cooperation with other agencies, has investigated cases in which government employees allegedly had improperly accessed and sold sensitive personal information that was then used by illegal immigrants to secure employment.

In addition, in 2005 FTC settled charges with BJ's Wholesale Club in which alleged security breaches resulted in several million dollars in fraudulent purchases using customers' credit and debit card data.[38] As discussed later in this report, FTC has also taken enforcement actions related to data breaches at several other companies, including ChoicePoint, CardSystems, and DSW, in which it uncovered evidence that the breaches resulted in identity theft.

Many of the law enforcement officials said that, based on their experience, data breaches that result in harm have usually involved fraud on existing accounts (such as credit card fraud) rather than the unauthorized creation of new accounts. Secret Service representatives noted that using illicit credit and debit card numbers and bank account information is much easier and less labor intensive than using personally identifiable information to fraudulently open new accounts. Officials at Secret Service, FBI, and USPIS all said that identity theft involving the creation of new accounts often results not from data breaches, but from other sources, such as retrieving personal information by sifting through a family's household trash.

In examining a selection of five breaches that occurred from 2003 through 2005 that were reported as having involved five federal agencies—Department of Justice, FDIC, Internal Revenue Service, National Park Service, and the Navy—we found that the circumstances behind these breaches varied widely. At least two of the breaches occurred at vendors or contractors that held sensitive data on agency employees, rather than at the agency itself. In addition, we found that a breach reported in the news media as having involved the National Park Service actually involved a not-for-profit organization that manages eParks, according to a representative of that organization. Four of the five breaches reported as having involved federal agencies were not believed to have resulted in identity theft, according to officials of the entities involved. The breach at

[38] *In the Matter of BJ's Wholesale Club, Inc.*, F.T.C. No. 0423160 (2005). A consent agreement does not constitute an admission of a violation of law.

FDIC resulted in an estimated 27 cases of identity theft when data inappropriately accessed by a former FDIC intern were used to take out more than $425,000 in fraudulent loans in the names of FDIC employees, according to agency officials.[39]

Industry and trade associations representing entities that maintain large amounts of information—banks, retailers, colleges, information resellers, and hospitals—told us that they had limited knowledge about the harm caused by data breaches that occur in their industries. However, in some cases, they provided information or anecdotal evidence on the extent to which such breaches may have led to some form of identity theft. For example, the 46 hospitals that the American Hospital Association surveyed at our request reported that of 17 breaches that had occurred since 2003, three had resulted in fraudulent activity on existing accounts and another three resulted in other forms of identity theft, including one case where the information was used to file false income tax refunds. The identity theft in these cases involved small numbers of victims—usually just one.

Representatives of the American Council on Education and two other higher education associations stated that while data breaches at colleges and universities were not uncommon, they were aware of little to no identity theft that had resulted from such breaches. Representatives of the American Bankers Association, the National Retail Federation, and the Consumer Data Industry Association told us they were unable to determine how prevalent data breaches are among their institutions or how often such breaches lead to consumer harm. Representatives at the National Retail Federation noted that breaches at retailers may be more likely to result in fraud on existing accounts than in new account creation, since most retailers do not maintain the personally identifiable information needed to steal someone's identity.

[39] According to an FDIC representative, the agency took several steps to address the possible misuse of employee information, including promptly notifying affected employees and offering them 2 years of credit monitoring services.

Of 24 Large Publicly Reported Breaches, 4 Apparently Resulted in Known Cases of Identity Theft

Using lists of data breaches compiled by the Identity Theft Resource Center, Privacy Rights Clearinghouse, and Congressional Research Service, we identified the 24 largest breaches (measured by number of records) that were reported in the news media from January 2000 through June 2005.[40] To gather information on these incidents, we interviewed or collected written responses from representatives of the entity experiencing the breach and reviewed publicly available information, such as media reports, news releases, testimonies, and court documents. In some cases, when feasible, we also spoke with law enforcement investigators. We identified those cases where this information collectively indicated that the breach appeared to have resulted in some form of identity theft. Ultimately, the determination of whether particular conduct violated a law prohibiting identity theft would be a matter of law for the courts.

Although these lists characterized each of these 24 incidents as data breaches, the circumstances of the incidents varied. While 19 of the incidents clearly met our definition of data breach (i.e. unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information), four cases involved hackers who may or may not have actually accessed sensitive information. In one other incident, a university employee with access to sensitive personal data was indicted on unrelated fraud charges. A university official told us he did not believe this incident should necessarily be characterized as a data breach since there was no evidence the employee actually misused university data.

The available evidence that we reviewed indicated that 18 of these 24 breaches were not known to have resulted in any identity theft. As shown in table 1, three breaches were believed to have resulted in account fraud and one resulted in the unauthorized creation of new accounts. In two

[40] These three organizations periodically update their lists by adding breaches they learn about that occurred in the past, including some that occurred between January 2000 and June 2005. Our list of the 24 largest media-reported breaches was based on information provided by these lists as of August 2006. We were not aware of the Attrition list at the time we made our selection. See Congressional Research Service, *Personal Data Security Breaches: Context and Incident Summaries*, Order Code RL33199 (Washington, D.C.: Dec. 16, 2005). Because our time frame covered only breaches that occurred on or before June 30, 2005, our list does not include highly publicized breaches that occurred subsequently, such as those involving the Department of Veterans Affairs and the TJX Companies. Several banks have reported fraudulent transactions on existing accounts resulting from the TJX breach, according to a January 24, 2007, press release by the Massachusetts Bankers Association.

other cases, we were not able to gather sufficient information on whether harm appeared to have resulted from the breach. Further, because of the challenges in linking data breaches with identity theft, in some cases our review may not have uncovered instances of harm potentially resulting from these breaches. In some instances, investigators or company representatives reported that they were able to determine with a high degree of certainty—through forensic investigation or other means—that unauthorized parties had not accessed the data. In other instances, these representatives said that they were not aware of any account fraud that resulted, but they acknowledged that there was no way to know for sure. Moreover, determining potential harm may be particularly challenging with very large breaches because the volume of records involved can make it difficult to link individual victims to the breach.

Table 1: Twenty-Four Large Publicly Reported Data Breaches and Evidence of Resulting Identity Theft, January 2000 - June 2005

Year[a]	Type of organization	Nature of breach	Available evidence of identity theft?[b]
2000	Retail	Hacking	Account fraud
2000	Retail	Hacking	None identified
2002	Healthcare	Stolen computer equipment	None identified
2003	Higher education	Stolen computer equipment	None identified
2004	Financial services	Stolen computer equipment	None identified
2004	Higher education	Hacking	None identified
2004	Higher education	Hacking	None identified
2004	Higher education	Hacking	None identified
2004	Financial services	Lost data tapes	None identified
2005	Financial services	Hacking	Account fraud
2005	State government	Hacking	None identified
2005	Information services	Deception/Misrepresentation	Unauthorized new accounts
2005	Higher education	Hacking	None identified
2005	Higher education	Stolen computer equipment	None identified
2005	Retail	Hacking	Account fraud
2005	Information services	Deception/Misrepresentation	Unknown
2005	Healthcare	Stolen computer equipment	None identified
2005	Retail	Hacking	Unknown
2005	Financial services	Lost data tapes	None identified
2005	Financial services	Employee crime	None identified
2005	State government	Hacking	None identified
2005	Media	Lost data tapes	None identified
2005	Financial services	Lost data tapes	None identified
2005	Higher education	Other[c]	None identified

Source: GAO.

Note: To identify the 24 largest data breaches reported in the news media from January 2000 through June 2005, GAO analyzed lists of such breaches maintained by Identity Theft Resource Center, Privacy Rights Clearinghouse, and Congressional Research Service.

[a] Year breach occurred or was publicized.

[b] The presence or lack of evidence of identity theft resulting from a breach was based on our review of news reports and other publicly available information, as well as interviews, as feasible, with representatives of entities experiencing the breach and law enforcement officials investigating the breach. The fact that we were unable to identify evidence at this time of identity theft resulting from a breach does not mean that no such harm has occurred or that none will occur in the future. Further, factual determinations of the existence and cause of identity theft in any particular case are matters for the courts to decide.

[c] In this case, a former university employee with access to sensitive personal information had been indicted on bank fraud charges unrelated to the university. Some press reports characterized this as a breach, but according to a representative of the university, there is no evidence that the employee misused university data.

The one large breach we identified that apparently resulted in the unauthorized creation of new accounts involved ChoicePoint, an information reseller. In 2005, the company acknowledged that the personal records it held on approximately 162,000 consumers had been compromised by individuals who posed as legitimate subscribers to the company's information services. FTC reached a civil settlement in 2006 with the company that established a fund for consumer redress to reimburse potential victims of identity theft, and the agency has worked with law enforcement officials to identify such victims.[41]

The three large breaches we identified that appeared to result in fraud on existing accounts included the following:

- CardSystems, a credit card payment processor, reported a May 2005 breach in which a hacker accessed data such as names, card account numbers, and expiration dates. The total number of compromised accounts is unclear. FTC staff alleged in a 2006 civil complaint that the breach had compromised data associated with tens of millions of credit and debit cards, but a CardSystems official stated in congressional testimony that only 239,000 accounts were compromised. Officials of the Office of the Comptroller of the Currency—who surveyed the national banks they supervise in order to determine the amount of fraudulent charges that resulted from the breach—said that customers of 110 banks were affected by this incident and losses of more than $13

[41] *United States v. ChoicePoint, Inc.*, No. 1:06-cv-00198-JTC (N.D. Ga., Feb. 15, 2006). As part of the settlement, ChoicePoint admitted no violations of the law. According to ChoicePoint, the company has subsequently taken steps to enhance its customer screening process and to assist affected consumers. FTC staff told us that law enforcement officials have determined that as many as 2,900 people have experienced the fraudulent creation of new accounts as a result of the breach. According to a ChoicePoint official, the criminal indictments indicated that 46 people may have been defrauded, but the accused individuals may not have used data acquired from ChoicePoint in all the crimes cited in the indictments.

million in fraudulent charges on customers' cards were reported by 24 of these institutions.

- DSW, a shoe retailer, said in an April 2005 news release that it had experienced a data breach in which a hacker accessed the names and card numbers associated with 1.4 million credit and debit card transactions at 108 of its stores, as well as checking account numbers and driver's license numbers from 96,000 check transactions. According to a complaint filed by FTC in March of 2006, there allegedly have been fraudulent transactions on some of these accounts.

- CD Universe, an Internet-based music store, reportedly experienced a breach in December 1999 in which a hacker accessed as many as 300,000 names, addresses, and credit card numbers from the company Web site, according to media reports and a company official. The hacker allegedly used some of the stolen credit card numbers to obtain money for himself.[42]

Challenges Exist in Determining the Link between Data Breaches and Identity Theft

Determining the link between data breaches and identity theft is challenging for several reasons. First, identity theft victims often do not know how their personal information was obtained. According to FTC, in approximately 65 percent of the identity theft complaints it received from October 1, 2005, through August 31, 2006, the victim did not know or report how the information was compromised. Second, victims may misattribute how their data were obtained. For example, federal officials and representatives of a private group that assists victims said that consumers who are notified of a breach often assume that any perceived mistakes on their credit card statements or credit report were a result of the breach. As a result, no government agency maintains comprehensive data on the underlying cause of identity theft. FTC told us that its Identity Theft Data Clearinghouse is limited to self-reported complaints and therefore does not contain statistically reliable information that would allow the agency to determine a link between data breaches and identity theft. Similarly, according to FBI, data maintained by the Internet Crime Complaint Center does not include information sufficient to determine the link between data breaches and identity theft.

[42] This breach occurred in December 1999 but was included in the 24 breaches we reviewed because it was reported in the media in January 2000.

Third, law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. Finally, conducting comprehensive studies of data breaches and identity theft can be hindered by issues of privacy and confidentiality. For example, companies that have experienced breaches may be unable or unwilling to provide information about affected individuals to researchers.

Some studies conducted by private researchers have sought to determine the extent to which data breaches result in identity theft, but our review found them to contain methodological limitations.[43] One research firm conducted a study of four data breaches, analyzing credit and other application data for suspicious relationships that indicated fraud.[44] The study estimated that no more than 0.10 percent of individuals whose data had been breached experienced resulting identity theft in the form of unauthorized new account creation. However, because the study reviewed only four data breaches, it cannot be considered representative of other breaches. Moreover, two of these breaches did not involve personally identifiable information and thus would not be expected to create a risk of fraud involving new account creation.

Another private research firm surveyed approximately 9,000 individuals about whether they had ever received a notification from an organization about the loss or theft of their personal information.[45] Of the approximately 12 percent of individuals who reported they had received such a notification, 3 percent—or 33 people—said they believed they had suffered identity theft as a result. However, these data are subject to limitations; among other things, individuals are often unaware of whether any fraud they have suffered was, in fact, due to a data breach. A third firm projected in a study that 0.8 percent of consumers whose information a

[43] Although we found limitations in how these studies linked data breaches and identity theft, we determined other aspects of these studies to be sufficiently reliable, and we refer to them elsewhere in this report.

[44] ID Analytics, Inc., *National Data Breach Analysis* (2006).

[45] Ponemon Institute, *National Survey* (2005). As noted earlier, this study may also be limited by a low survey response rate.

data breach compromised would experience fraud as a result.[46] However, we question the reliability of this estimate, in part because of assumptions made about the number of consumers affected by data breaches.

Type of Data Compromised and Other Factors Influence Potential for Resulting Consumer Harm

The type of data compromised in a breach can effectively determine the potential harm that can result. For example, credit or debit card information such as card numbers and expiration dates generally cannot be used alone to open unauthorized new accounts. Some of the largest and most highly publicized data breaches in recent years largely involved credit or debit card data rather than personally identifiable information. As a result, these breaches put affected consumers at risk of account fraud but not necessarily at risk of fraud involving unauthorized creation of new accounts—the type of identity theft generally considered to have a more harmful direct effect on consumers. While credit and debit card fraud is a significant problem—the FTC estimates it results in billions of dollars in losses annually—existing laws limit consumer liability for such fraud and, as a matter of policy, some credit and debit card issuers may voluntarily cover all fraudulent charges.[47] In contrast, the unauthorized creation of new accounts—such as using someone else's identity to open credit card or bank accounts, originate home mortgages, file tax returns, or apply for government benefits—can result in substantial financial costs and other hardships.

In addition to the type of data compromised in a breach, several additional factors can influence the extent to which a breach presents the risk of identity theft. These include the following:

- *Intent.* Breaches that are the result of intentional acts—such as hacking into a server to obtain sensitive data—generally are considered to pose more risk than accidental breaches such as a lost laptop or the

[46] Javelin Strategy & Research, *Data Breaches and Identity Fraud: Misunderstanding Could Fail Consumers and Burden Businesses* (Pleasanton, California, August 2006).

[47] For unauthorized credit card charges, consumer liability is limited to a maximum of $50 per account, 15 U.S.C. § 1643. For unauthorized ATM or debit card transactions, the Electronic Fund Transfer Act limits consumer liability, depending on how quickly the consumer reports the loss or theft of the card. Pub. L. No. 90-321, tit. IX, as added Pub. L. No. 95-630, tit. XX, § 2001, 92 Stat. 3728 (Nov. 10, 1978); 15 U.S.C. § 1693g. Consumers may incur additional costs if they inadvertently pay charges they did not incur. In addition, account fraud can cause inconvenience or temporary hardship—such as losing temporary access to account funds or requiring the cancellation and reactivation of cards and the redirecting of automatic payments and deposits.

unintentional exposure of sensitive data on the Internet, according to federal agency officials. However, in some cases, such as the theft of a laptop containing personal information, it may be unknown whether the laptop was stolen for the hardware, the personal data, or both.

- *Encryption*. Encryption—encoding data so that it can only be read by authorized individuals—can in some cases prevent unauthorized access. However, some forms of encryption are more effective than others, and encryption does not necessarily preclude fraudulent use of data—for example, if the key used to unencrypt the data is also compromised.

- *Hardware requirements*. Data that only can be accessed using specialized equipment and software may be less likely to be misused in the case of a breach. For example, some entities that have lost data tapes have stated that criminals would require specific data reading equipment and expertise in how to use it to access the information.

- *Number of records*. Larger breaches may pose a greater overall risk that at least one individual would become a victim of identity theft. At the same time, given the resources needed to commit identity theft, breaches of very large numbers of records may pose less risk to any one individual whose data were compromised.

Breach Notification Requirements Can Serve to Encourage Better Data Security Practices and Alert Consumers, but They Also Present Costs and Challenges

Breach notification requirements have several potential benefits, including creating incentives for entities to improve their data security practices (and thus prevent potential breaches from occurring), allowing affected consumers to take measures to prevent or mitigate identity theft, and serving to respect individuals' basic right to know when their personal information is compromised. At the same time, breach notification requirements present costs, both for developing compliance strategies and for actual notifications in the event of a breach. Further, there is the risk of overnotification, or inundating consumers with frequent notifications of breaches that may present little or no risk of identity theft or other harm. Thus, policymakers face the challenge of setting a notification standard that allows individuals to take steps to protect themselves where the risk of harm exists, while ensuring they are only notified in cases where the level of risk warrants such action.

Notification Requirements May Create Incentives for Improved Data Security and Allow Consumers the Opportunity to Mitigate Risks

According to our review of studies and interviews with representatives in government, academia, and private industry, breach notification requirements have several potential benefits, as follows:

- *Incentives for Improved Data Security.* Breach notification requirements can provide an incentive for companies and other entities to increase their data security measures to avoid the possible financial and reputational risks that can be associated with a publicly reported data breach.[48] Representatives we contacted in the private, nonprofit, and government sectors told us that they believe that existing breach notification requirements in state laws, or the breach notification provisions in federal banking regulatory guidance, have provided entities with incentives to improve data security practices. For example, some representatives of companies and other organizations noted that passage of state notification laws led to companies reexamining data security procedures and making improvements, such as encrypting sensitive data and restricting consumer data that can be accessed online. Similarly, federal banking regulators told us that they believe their notification guidance has motivated regulated institutions to enhance data security. For example, according to officials at the Office of Thrift Supervision, its institutions have taken steps such as improving electronic firewalls and implementing formal incident response reporting systems.

- *Prevention of Identity Theft.* Breach notification can provide consumers with the opportunity to take steps to protect themselves from possible identity theft. For example, consumers whose account information has been breached can monitor their bank or credit card statements for suspicious activity or close the affected accounts. Consumers whose personally identifiable information, such as SSN, has been breached can review their credit reports for suspicious activity or may choose to purchase a credit monitoring product that alerts them to changes that could indicate identity theft. In addition, affected consumers can place a fraud alert on their credit reports, which requires businesses to take certain identity verification steps before

[48] Such costs can be significant. For example, according to a 2006 survey, 31 companies that responded to the survey incurred an average of $98 per record, or $2.6 million per company, in costs associated with the loss of existing customers, recruitment of new customers, and damage to the reputation of their brand name. Ponemon Institute, LLC, *2006 Annual Study: Cost of a Data Breach*, 2006. Due to sampling limitations, these findings are not necessarily representative of the costs incurred by all companies that experience breaches.

issuing credit.[49] In some states, consumers can implement credit freezes, which block unauthorized third parties from obtaining the consumer's credit report or score.[50] Limited information exists on the steps individuals actually take when notified of a breach. In the 2005 Ponemon Institute survey of individuals that received notification letters, 50 percent said they did nothing, while the rest indicated they took actions such as monitoring their credit reports, canceling credit or debit cards, or closing bank accounts.[51]

- *Respecting Consumers' Right to Know*. Some consumer advocates and others have argued that consumers have a right to know how their information is being handled. According to this view, basic rights of privacy dictate that consumers should be informed when their personal information has been compromised, even if the risk of harm is minimal. The principle that individuals should have ready means of learning about the use of their personal information is embedded in the Fair Information Practices, a set of internationally recognized privacy protection principles.[52]

- *Improving Public Awareness*. Public reporting of data breaches may raise general awareness among consumers about the risks of identity theft and ways they can mitigate these risks, such as periodically reviewing their credit reports. In addition, publicity surrounding a data breach resulting from notification can serve to deter the use of stolen information because presumably the thief knows that the breach is likely being investigated and the stolen data are being carefully monitored.

[49] *See* 15 U.S.C. § 1681c-1.

[50] Congressional Research Service, *Identity Theft Laws: State Penalties and Remedies and Pending Federal Bills* (Washington, D.C.: Jan. 11, 2007).

[51] Ponemon Institute, *National Survey* (2005). As noted earlier, this study may be limited by a low survey response rate.

[52] The Fair Information Practices were first proposed in 1973 by a U.S. government advisory committee. A revised version was developed in 1980 by the Organization for Economic Cooperation and Development, a group of 30 member countries that are market democracies. For more information, see GAO, *Personal Information: Agency and Reseller Adherence to Key Privacy Principles*, GAO-06-421 (Washington, D.C.: Apr. 4, 2006).

Breach Notification Requirements Present a Variety of Potential Costs

According to company representatives, researchers, regulators, and others, there are several different types of costs that may be associated with breach notification requirements. To begin with, entities subject to breach notification requirements may incur certain costs, regardless of whether they actually suffer a breach, or—if they do—regardless of whether they have to notify consumers. For example, entities may incur costs for developing and formalizing incident response plans.

There are also the costs associated with actual notifications—potentially including printing, postage, legal, investigative, and public relations expenses.[53] Although comprehensive data on these costs do not exist, a 2006 Ponemon Institute survey of companies experiencing a data breach found that 31 companies that responded incurred an average of $1.4 million per breach, or $54 per record breached, for costs related to mailing notification letters, call center expenses, courtesy discounts or services, and legal fees.[54] Similarly, a study by Gartner Research found that ChoicePoint spent $79 per affected account following its 2005 breach for professional fees, legal expenses, and communications to affected customers.[55] A representative of the San Jose Medical Group told us it spent $100,000 to send notification letters to 187,000 patients following a data breach that occurred in 2005. Entities also may incur costs related to staffing call centers to field inquiries from consumers about the breach. For example, representatives of the University of California at Berkeley told us that following a 2005 breach of 98,000 records, the university spent $75,000 in staffing, telecommunications, and other call center costs.

Finally, banks whose customers' account information is breached also may incur costs for remedial steps such as canceling existing accounts or replacing affected customers' credit or debit cards—although such steps may not be required by the applicable breach notification requirements.

[53] The distinction between the costs associated with a notification requirement versus a breach itself can be ambiguous. For example, the cost of postage can clearly be attributed to notification, whereas legal costs can be attributed to notification, the breach itself, or both, depending on the circumstances.

[54] Ponemon Institute, *Annual Study* (2006). As noted earlier, due to sampling limitations, these findings are not necessarily representative of the costs incurred by all companies that experience breaches.

[55] Gartner Research, *Data Protection Is Less Costly Than Data Breaches* (Stamford, Connecticut: September 16, 2005). The report, issued in 2005, based its findings on the breach having affected 145,000 records, but company officials later reported that 162,000 records were affected.

Entities experiencing a breach also often provide affected individuals with free credit monitoring services. For example, a representative of a large financial management company noted that offering free credit monitoring services after a breach has become standard industry practice, and costs, on average, between $20 and $40 per customer.

Challenges Exist in Complying with and Developing Breach Notification Requirements

Officials of companies and other entities we interviewed identified challenges such as interpreting ambiguous statutory language, identifying and locating affected consumers, and developing effective notification letters. In addition, policymakers face challenges in developing breach notification requirements, particularly in setting the appropriate standard to establish the circumstances under which consumers should be notified.

Complying with Notification Requirements

Companies and other entities we interviewed said they can face a number of challenges related to complying with the breach notification requirements in state laws or federal banking guidance. These include the following:

- *Interpreting ambiguous provisions.* Entities subject to breach notification requirements sometimes face challenges interpreting certain terms or provisions of notification laws. For example, an information security expert told us that some laws do not adequately define encryption, which could refer to anything from simple password protection to complex coding. Similarly, federal banking regulators acknowledged that their institutions sometimes face difficulty determining whether misuse of breached information is “reasonably possible,” such as when little information exists about the location of the data, the intent of a criminal who stole data, or the effectiveness of security features designed to render data inaccessible.

- *Addressing who is responsible.* Notification requirements do not always fully address who should bear the cost of and responsibility for notification, particularly in cases where a third party is responsible for the breach. For example, representatives of some federal banking regulators and industry associations cited particular challenges associated with breaches of credit and debit card information by retailers. Banks that issue credit and debit cards compromised by a merchant that is not the bank’s service provider are generally not required by the banking regulators’ guidance to notify their customers, but nevertheless in some cases, they feel obliged to do so. Bank representatives with whom we spoke expressed concern that breaches of credit card information by third parties can adversely affect a bank’s reputation and result in costs related to notifying customers and reissuing cards.

- *Identifying affected consumers*. Some entities we interviewed said that it can be difficult to identify which consumers may have been affected by a breach and obtain their contact information. For example, one representative at a state agency involved in a breach told us officials were unsure what data had been downloaded among records that may have been accessed on 600,000 people. Obtaining accurate and current mailing addresses for affected parties also can be difficult and costly, many entities told us. This can be a particular problem for entities, such as merchants, that have breached credit card numbers but do not themselves possess the mailing addresses associated with those numbers.

- *Developing clear and effective notification letters*. We have noted in the past that public notices should be useful and easy to understand if they are to be effective.[56] However, the 2005 study conducted by the Ponemon Institute found that 52 percent of survey respondents who received a notification letter said the letter was not easy to understand.[57] In addition, consumers might be confused by other mail solicitations that may resemble notification letters. For example, officials at one large national bank noted that marketing solicitations for credit monitoring services often are made to resemble breach notification letters, potentially desensitizing or confusing consumers when a true notification letter arrives.

- *Complying with multiple state laws*. Officials of companies with customers in multiple states and their trade associations noted that they face the challenge of complying with breach notification requirements that vary among the states, including who must be notified, the level of risk that triggers a notice, the nature of the notification, and exceptions to the requirement. Officials of companies we contacted noted that it is challenging to comply with these multiple requirements since most breaches involve customers in many states.

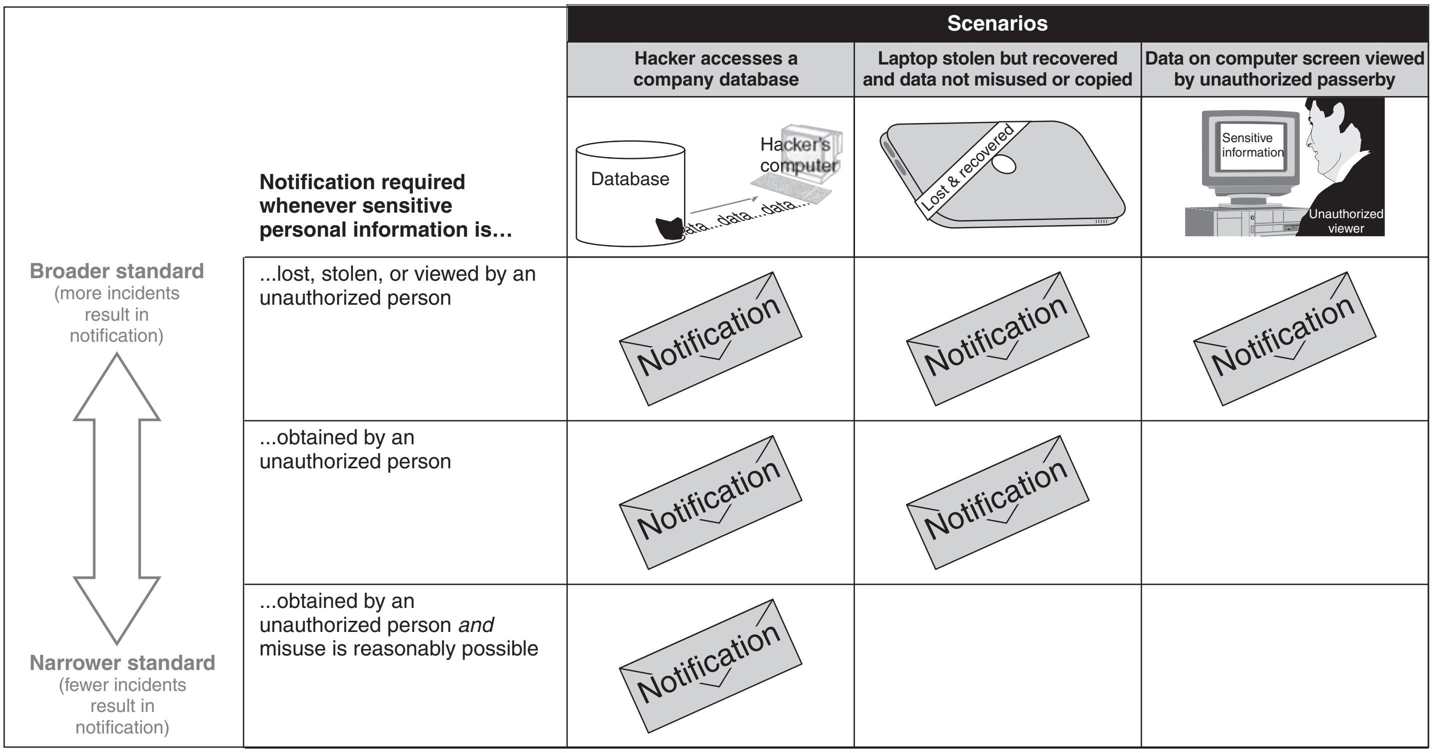
[56] *See* GAO-06-833T, *Privacy: Preventing and Responding to Improper Disclosures of Personal Information* (Washington, D.C.: Jun. 8, 2006), pp. 15-18, which discusses specific elements that should be incorporated in a breach notification.

[57] Ponemon Institute, *National Survey* (2005). As noted earlier, this study may be limited by a low survey response rate.

Setting an Appropriate Notification Standard

Existing state laws vary in terms of the notification standard—that is, the event or circumstance that triggers a required notification. For example, California has an expansive standard that requires notification in nearly all cases where unencrypted sensitive personal data "is reasonably believed to have been acquired by an unauthorized individual." Other states employ a risk-based approach that incorporates into the standard the extent to which the data are likely to be misused. The standards vary in terms of what is required in cases where the risk of harm is unknown. For example, Vermont requires notification unless an entity can demonstrate that misuse of the breached data "is not reasonably possible." In contrast, North Carolina requires notification only when it has been determined that the breach has resulted, or is reasonably likely to result, in illegal use of the data or creates a material risk of harm to a consumer. As shown in figure 1, whether or not a breach is subject to notification can depend on the specific notification standard.

Figure 1: Application of Notification Standards under Different Breach Scenarios



	Notification required whenever sensitive personal information is…	Scenarios: Hacker accesses a company database	Scenarios: Laptop stolen but recovered and data not misused or copied	Scenarios: Data on computer screen viewed by unauthorized passerby
Broader standard (more incidents result in notification)	...lost, stolen, or viewed by an unauthorized person	Notification	Notification	Notification
	...obtained by an unauthorized person	Notification	Notification	
Narrower standard (fewer incidents result in notification)	...obtained by an unauthorized person *and* misuse is reasonably possible	Notification		

Source: GAO (analysis); Art Explosion (images).

Note: Figure presents hypothetical scenarios and notification standards and is shown for illustrative purposes only.

Because of the difficulty of complying with multiple state requirements, many companies and industry representatives have argued for a consistent federal standard for breach notification that would preempt state notification laws. However, the National Association of Attorneys General, as well as some consumer and privacy groups, have expressed concern that a federal breach notification law could weaken consumer protections if it were to preempt stronger state laws. These groups have advocated a strong notification standard because, they say, the link between breaches and identity theft is not always clear and entities are not well equipped to assess the risk of harm resulting from a given breach. As a result, too narrow a notification standard may prevent consumers from taking action in cases that do in fact present some risk. Also, as noted earlier, some privacy groups and others believe that consumers have basic rights to be notified when their personal information has been breached, no matter what the circumstances. Moreover, they say that fears of "overnotification"—where consumers are inundated by frequent notifications—are unfounded, given that they are aware of no evidence of this occurring in states that currently have strict notification requirements.

By contrast, some representatives of the federal banking regulatory agencies, FTC, private companies, and other experts have expressed concern about overly expansive breach notification standards. They say that such standards may require businesses to notify consumers about minor and insignificant breaches. This in turn could eventually lead to overnotification and cause consumers to spend time and money taking proactive steps that are not necessary or, alternatively, to ignore notices when action is warranted. In addition, businesses and federal banking regulators have expressed concern about the financial burden that overnotification could cause. Overly broad notification standards could also have the effect of limiting entities' reputational incentives for improving data security, if nearly all entities regularly issue notifications as a result of minor breaches. Representatives of the federal banking regulatory agencies have noted that they sought to strike an appropriate balance with their notification standard. Their guidance provides that, when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused.[58] If the institution determines that

[58] 12 C.F.R. Pt. 30, App. B, Supp. A § III(A); 12 C.F.R. Pt. 208, App. D-2, Supp. A § III(A); 12 C.F.R. Pt. 225, App. F, Supp. A § III(A); 12 C.F.R. Pt. 364, App. B, Supp. A § III(A); 12 C.F.R. Pt. 570, App. B, Supp. A § III(A); and 12 C.F.R. Pt. 748, App. B § III(A).

misuse of the information has occurred or is reasonably possible, it should notify affected customers as soon as possible. The guidance is intended to provide notice to customers only when there is a reasonable expectation of misuse.[59]

Similarly, the guidance for federal agencies developed by the President's Identity Theft Task Force recommended that if an agency experiences a breach, it should analyze the risk of identity theft and tailor its response—which may include notifying individuals—to the nature and scope of the risk presented. The guidance noted that such a risk assessment can minimize the potentially significant costs of notification where little risk exists. The task force's April 2007 strategic plan recommended the development of a national standard requiring all entities that maintain sensitive consumer information, in both the public and private sectors, to provide notice to consumers and law enforcement in the event of a breach. As with its guidance to federal agencies, the task force recommended that the standard be risk based to provide notice when consumers face a significant risk of identity theft but to avoid excessive notification.

As we have noted in the past, care is needed in defining appropriate criteria for data breaches that merit notification.[60] The frequency of data breaches identified in this report suggests that a national breach notification requirement may be beneficial, in large part because of its role in further encouraging entities to improve their data security practices. However, because breaches vary in the risk they present, and because most breaches have not resulted in detected incidents of identity theft, a notification that is risk based appears appropriate. Should Congress choose to enact a federal breach notification requirement, use of the risk-based approaches that the federal banking regulators and the President's

[59] The guidance states that institutions should notify their primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, even for incidents that may not warrant customer notification. Banking regulators told us they review institutions' response programs as part of their supervisory procedures and, in many cases, work with institutions as they respond to specific incidents to ensure their actions are in accordance with the guidance. *See* 12 C.F.R. Pt. 30, App. B, Supp. A § II(A)(1)(b); 12 C.F.R. Pt. 208, App. D-2, Supp. A § II(A)(1)(b); 12 C.F.R. Pt. 225, App. F, Supp. A § II(A)(1)(b); 12 C.F.R. Pt. 364, App. B, Supp. A § II(A)(1)(b); 12 C.F.R. Pt. 570, App. B, Supp. A § II(A)(1)(b); and 12 C.F.R. Pt. 748, App. B § II(A)(1)(b).

[60] GAO, *Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data*, GAO-06-674 (Washington, D.C.: Jun. 26, 2006) and GAO-06-833T.

Identity Theft Task Force advocate could avoid undue burden on organizations and unnecessary and counterproductive notifications to consumers.

Agency Comments

We provided a draft of this report to FTC, which provided technical comments that were incorporated in this report as appropriate. In addition, we provided selected portions of the draft to the Board of Governors of the Federal Reserve System, the Department of Justice, DHS, FDIC, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Social Security Administration, and USPIS, and also incorporated their technical comments as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. We will then send copies of this report to the Chairman, House Committee on Financial Services; the Chairman and Ranking Member, Senate Committee on Banking, Housing, and Urban Affairs; the Chairman and Ranking Member, Senate Committee on the Judiciary; the Chairman and Ranking Member, House Committee on the Judiciary; the Chairman and Vice Chairman, Senate Committee on Commerce, Science, and Transportation; and the Chairman and Ranking Member, House Committee on Energy and Commerce. We will also send copies to the Chairman of the Board of Governors of the Federal Reserve System, the Attorney General, the Secretary of the Department of Homeland Security, the Chairman of the Federal Deposit Insurance Corporation, the Chairman of the Federal Trade Commission, the Chairman of the National Credit Union Administration, the Comptroller of the Currency, the Director of the Office of Thrift Supervision, the Commissioner of the Social Security Administration, and the Postmaster General and Chief Executive Officer of the U.S. Postal Service. We will also make copies available to others upon request. In addition, the report will be available at no charge on GAO’s Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-8678 or woodd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.

David G. Wood

David G. Wood
Director, Financial Markets and
Community Investment

Our report objectives were to examine (1) what is known about the incidence and circumstances of breaches of sensitive personal information; (2) what information exists on the extent to which breaches of sensitive personal information have resulted in identity theft; and (3) the potential benefits, costs, and challenges associated with breach notification requirements. We use the term "data breach" to refer to the unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information by a company, government agency, university, or other public or private entity. Our scope was limited to breaches involving personal data, including financial data, that could be used to commit identity theft or other related harm, and we excluded breaches involving other types of sensitive data, such as medical records or proprietary business information. For the purposes of this report, the term "identity theft" is used broadly to refer to both fraud on existing accounts and the unauthorized creation of new accounts.

To address all three objectives, we conducted a literature search of relevant articles, reports, and studies. We also collected and analyzed documents from, and interviewed, officials of government agencies that investigate and track data breaches, including the Federal Trade Commission, the Department of Homeland Security, the Department of Justice, the U.S. Postal Inspection Service, and the Social Security Administration. We also interviewed staff at the five federal banking regulators—the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration. In addition, we spoke with representatives of the National Association of Attorneys General and organizations that address consumer protection and privacy issues, including Consumers Union, Electronic Privacy Information Center, Privacy Rights Clearinghouse, Attrition, and the Identity Theft Resource Center. We also spoke with three academic researchers who study issues related to data breaches and notification and an attorney who helps companies address data privacy and security issues. In addition, we reviewed studies on data breaches conducted by private and nonprofit research organizations, including the Ponemon Institute, ID Analytics, and Javelin Strategy and Research. We interviewed the studies' authors and took other steps to ensure that the data and methodologies were sufficiently reliable for our purposes. We also spoke with representatives of the California Office of Privacy Protection and its advisory group and reviewed the office's recommended practices for notification.

To address the first objective on the incidence and circumstances of data breaches, we reviewed lists of news media-reported data breaches that are compiled and maintained by three private research and advocacy organizations—Privacy Rights Clearinghouse, Attrition, and the Identity Theft Resource Center. We analyzed the three independent lists to create a single, nonduplicative list of data breaches that had been reported in the news media from January 2005 through December 2006. We took measures to ensure the lists were of sufficient quality for our purposes, including spot checking selected data and interviewing representatives of the three organizations on their methodologies. The Privacy Rights Clearinghouse, Attrition, and Identity Theft Resource Center lists contained 436, 453, and 462 breaches, respectively, for the time period we analyzed. Of the 572 breaches they collectively compiled, 59 percent appeared on all three lists, 19 percent appeared on two, and 22 percent appeared on one. Our analysis was based on the lists as they stood on February 15, 2007; these data may have changed because the lists are occasionally updated when the compilers learn of new breaches that may have occurred in the past.

We also collected available data from federal law enforcement agencies on the breaches they have investigated in recent years. In addition, the five federal banking regulators provided, at our request, data on the breaches of which they have been notified by the institutions they supervise. These data varied in usefulness and comprehensiveness because of the regulators' differing methods of counting and tracking breaches and maintaining data on them. We also gathered data from two states, New York and North Carolina, which were selected because they were two large states that maintain centralized information on breaches. Further, we obtained available data from industry and trade associations representing key sectors—such as financial services, retail sales, higher education, hospitals, and information services—that have experienced data breaches. We also collected information on breaches experienced by federal agencies compiled by the House Government Reform Committee and the U.S. Computer Emergency Readiness Team, a component of the Department of Homeland Security.

To address the second objective, we selected for more detailed examination the 24 largest (in terms of number of records breached) data breaches reported in the news media from January 2000 through June 2005. We selected these breaches in August 2006 using the lists maintained by Privacy Rights Clearinghouse and Identity Theft Resource Center, as well as a similar compilation of breaches collected by the Congressional Research Service. We were not aware of the Attrition list at the time we made our selection. For each of these breaches, we reviewed news reports as well as publicly available documents such as testimonies and criminal indictments. We also conducted interviews, where possible, with representatives of the entities that experienced the breach and law enforcement agencies that investigated the breach. We identified those cases where this information collectively indicated that the breach appeared to have resulted in some form of identity theft. Ultimately, the determination of whether particular conduct violated a law prohibiting identity theft would be a matter of law for the courts. We did not directly contact individuals whose data had been affected by the breaches because of privacy concerns and because we did not have a systematic means of identifying them. We also reviewed five breaches that reportedly involved federal agencies—the Navy; the Internal Revenue Service; the Federal Deposit Insurance Corporation; the National Park Service; and the Department of Justice. These were selected to represent breaches that included different causes, types of data, and involvement by third-party vendors.

To examine the potential benefits, costs, and challenges associated with breach notification requirements, we reviewed the federal banking regulators' proposed and final guidance related to breach notification, and interviewed representatives of each agency regarding their consideration of potential costs, benefits, and challenges during development of the guidance. Further, we reviewed the strategic plan and other documents issued by the President's Identity Theft Task Force. In addition, we conducted a review of the effects of California's breach notification law. We interviewed representatives of, and gathered information from, seven organizations to learn about their experiences complying with California's breach notification law. These organizations were selected to represent a range of organization sizes and industry sectors. We also interviewed representatives of the California State Information Security Office, California State Assembly, California Office of Privacy Protection, and California Bankers Association.

We conducted our review from August 2006 through April 2007 in accordance with generally accepted government auditing standards.

GAO Contact

David G. Wood, (202) 512-8678 or woodd@gao.gov

Staff Acknowledgments

In addition to the contact named above, Jason Bromberg, Assistant Director; Randy Fasnacht; Marc Molino; Kathryn O'Dea; Carl Ramirez; Linda Rego; Barbara Roesmann; and Winnie Tsen made key contributions to this report.

(250295)

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON ♲ RECYCLED PAPER

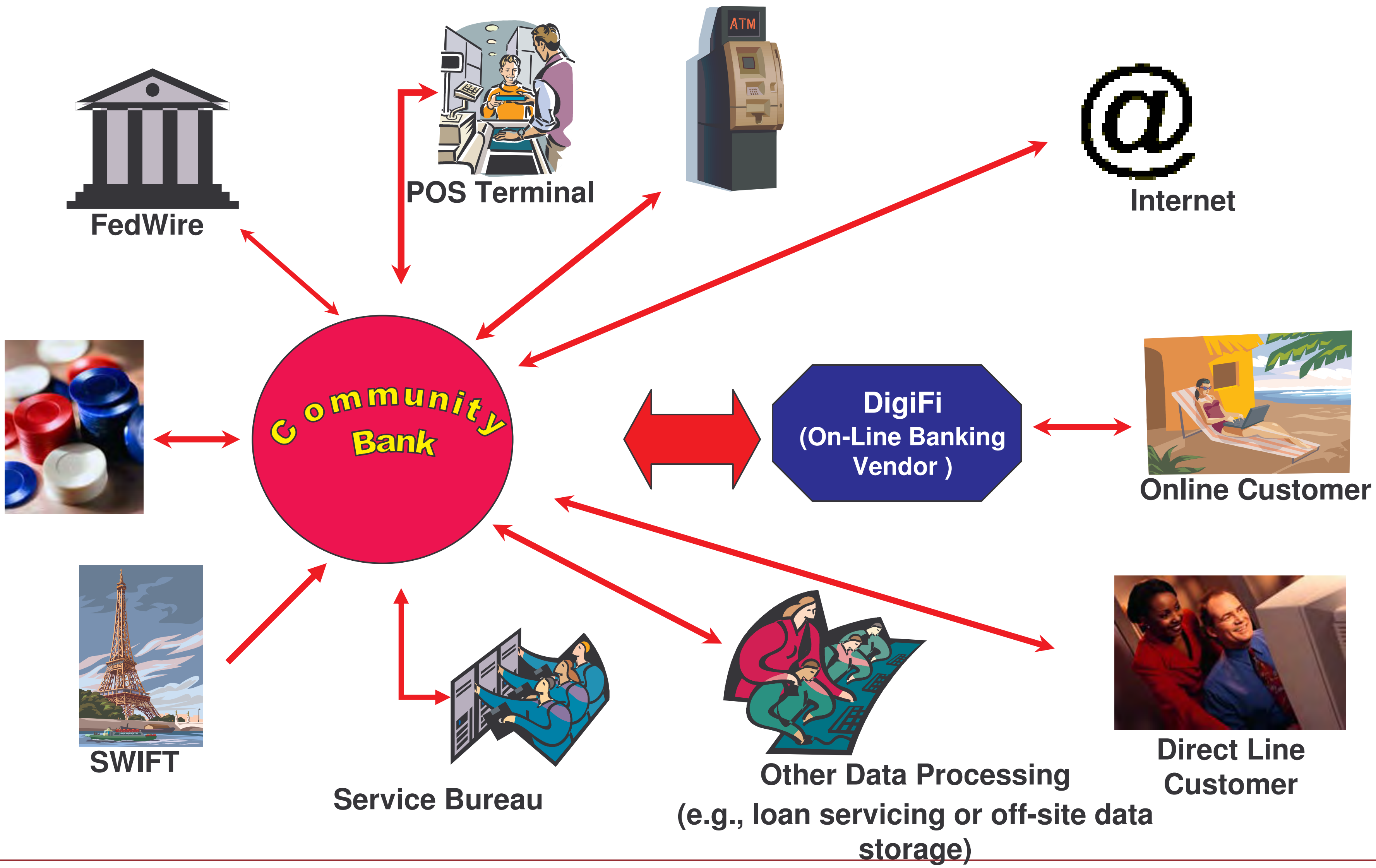
All Roads Lead to Rome: The Origins of the Digital Insider

Tom Kellermann, CISM / SVP of Security Awareness ,
Core Security Technologies

History Repeats Itself

- Hannibal using the Roman Roads to cross the Alps

Computers and The Internet



Reality Check

- There has been a 40 percent increase in intrusions into U.S. government networks.

  -*US-CERT, 2008*

- **56,000** instances of wire transfer fraud in the financial sector since 1997, **more than half have occurred in the past two years.** -*FINCEN, 2009*

Sun Tzu

- **Sun Tzu:** “It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.”

Setting the Table

- Cyber-attacks have become a wholly pervasive phenomenon based in part on:
  - Increasing connectivity and availability of assailable network, systems and applications vulnerabilities.
  - The ability of cybercriminals to derive significant financial rewards through successful attacks.
  - Worldwide federation between various classes of cyber-criminals and malware developers.
  - Nation-state, terrorist and politically-driven backing of targeted cybercrime efforts.
  - A lack of cohesive law enforcement around the globe.

Botnet Zombies Taking Over

- Fourteen million PCs were compromised by botnet malware in Q2 2009, driving spam and malware to their highest levels ever, a 16% increase over Q1.

- *Some 150,000 new computers were infected by botnet programs each day, or 20% of PCs that are purchased.*

- As the number of bots continues to grow, malware writers have begun to offer malicious software as a service to back those who control botnets.

-*McAfee AVERT Labs research Reports*, 2009

I. Online Attacks Dominate

- A new malware infection site is discovered every 4.5 seconds, 24 hours a day, 365 days a year.

- Of the affected Web pages, 85% are on legitimate Web sites that have been hacked.

- The U.S. led the world in hosting just under three in every eight infected Web pages in 2008, an increase over 2007, when it had under 25%.

-*Sophos Security Threat Report*, 2009

Real Cyber-Warfare Battles

HE'S GONE: Jerry Garcia Dead at 53
TIME
CYBER WAR
The U.S. rushes to turn computers into tomorrow's weapons of destruction. But how vulnerable is the home front?

-Some 108 countries with dedicated cyber attack capabilities (FBI 2007)

-Russia-based attacks on Estonian Web assets.

-Coordinated attacks against Internet infrastructure of Georgia.

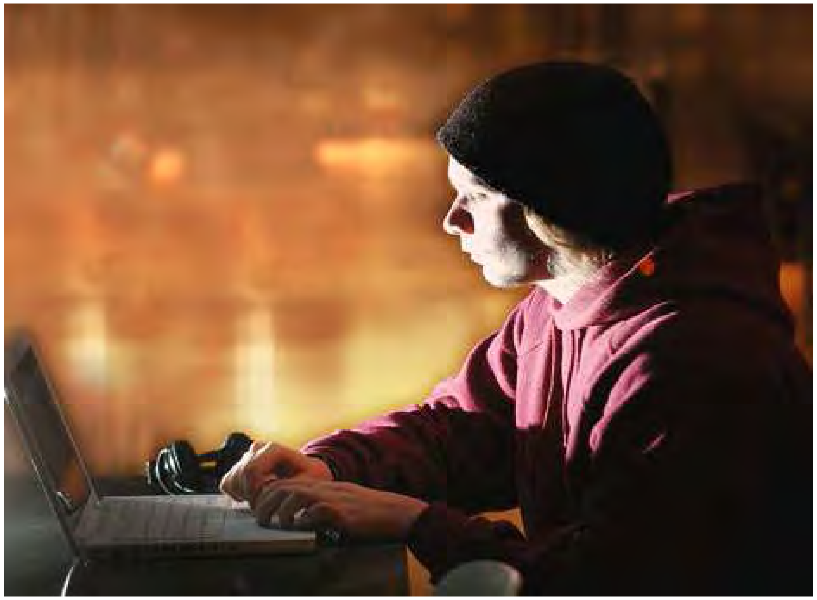
-Congressional demand for increased U.S. cyber-war preparedness/capabilities.

Empowering Non-State Actors

- The Internet is a true force mobilizer - and a thus force multiplier - for non-state actors.
  - Recruitment tool
  - Propaganda tool
  - Communication medium
  - Financing tool
  - Money laundering mechanism
  - Attack vector

Organized Data Thieves Running Wild

- Organized cyber-criminals are using sophisticated, targeted attacks to steal mountains of consumer records.



Shadow Economy

- 50,000 new instances of malware released daily.
- Age of the "Cyber Dons"
- Russian business network-CREWS
- Marketplace: primary commodities

  1) Bank logins

  2) Confidential customer information

  3) Credit card data

  4) Compromised machines

  5) Zero-day exploit code

Cybercrime is FBI's #1 criminal priority

Modern Maginot Lines

- Early 1990s: Virus scanners
- Mid 1990s: Firewalls
- Late 1990s: Over-reliance on encryption (PKI)
- Early 2000s: Over-reliance on IDS
- Late 2000s: Over-reliance on intrusion prevention systems / artificial intelligence

Know yourself…

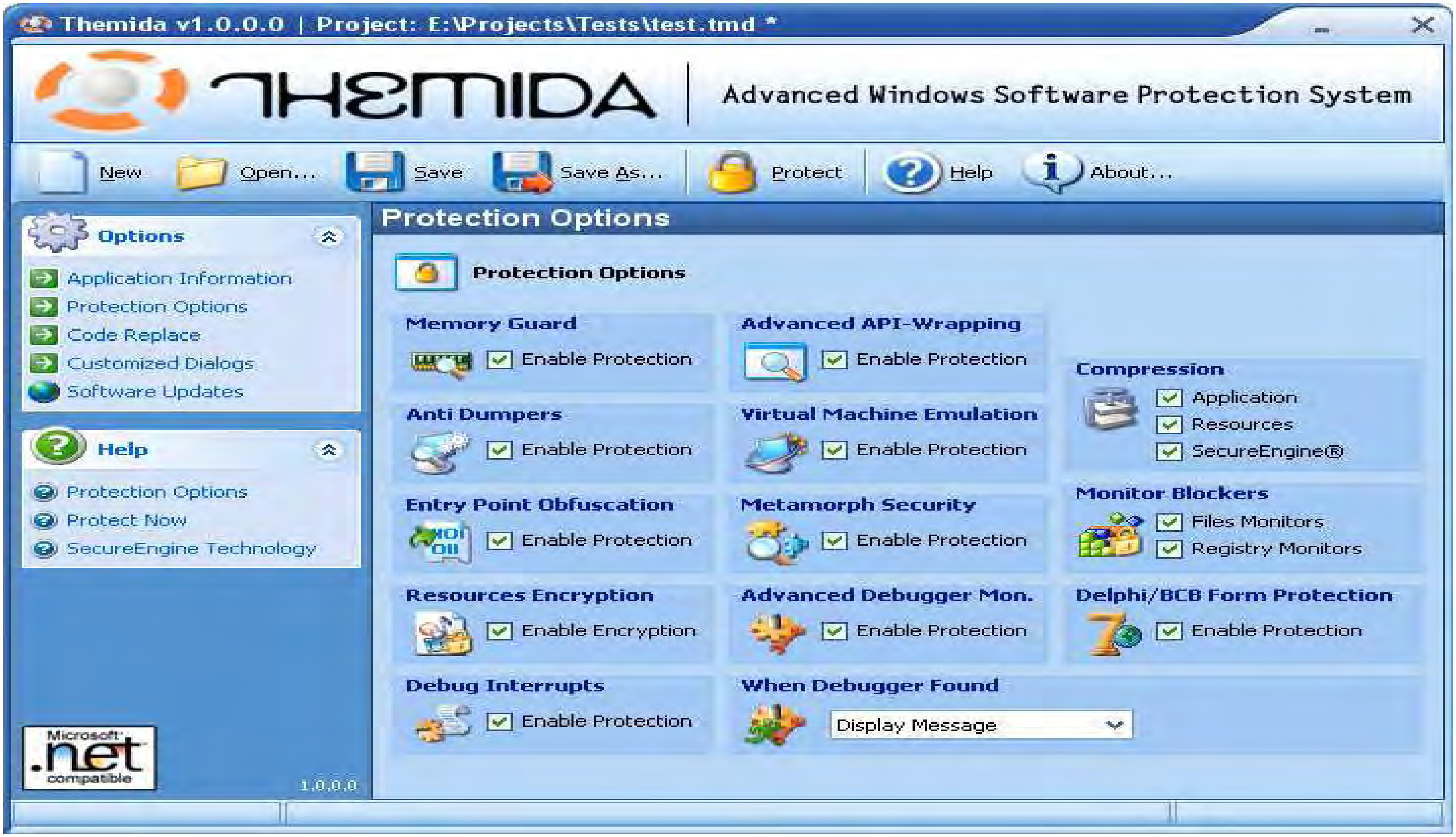
2009 Trends in Attacks Against .GOV

- SQL Injection and Cross-site Scripting
- Island Hopping
- Remote User Compromise-VPN Attacks-Client Side Attacks
- PKI Compromise -- Private Key Theft
- Zero-Day Attacks
- Digital Insider Attacks

Primary Attack Vectors

- Digital insider attacks previously compromised systems
- Client-side applications (applications running on desktop / end-user systems, including email readers, web browsers, media players, instant messengers, productivity tools such as MS Office, etc.)
- Operating systems
- Web applications
- Wireless networks

Themida Protector



Protection Options

Protection Options

Memory Guard
☑ Enable Protection

Advanced API-Wrapping
☑ Enable Protection

Compression
☑ Application
☑ Resources
☑ SecureEngine®

Anti Dumpers
☑ Enable Protection

Virtual Machine Emulation
☑ Enable Protection

Entry Point Obfuscation
☑ Enable Protection

Metamorph Security
☑ Enable Protection

Monitor Blockers
☑ Files Monitors
☑ Registry Monitors

Resources Encryption
☑ Enable Encryption

Advanced Debugger Mon.
☑ Enable Protection

Delphi/BCB Form Protection
☑ Enable Protection

Debug Interrupts
☑ Enable Protection

When Debugger Found
Display Message

Advanced Persistent Threat

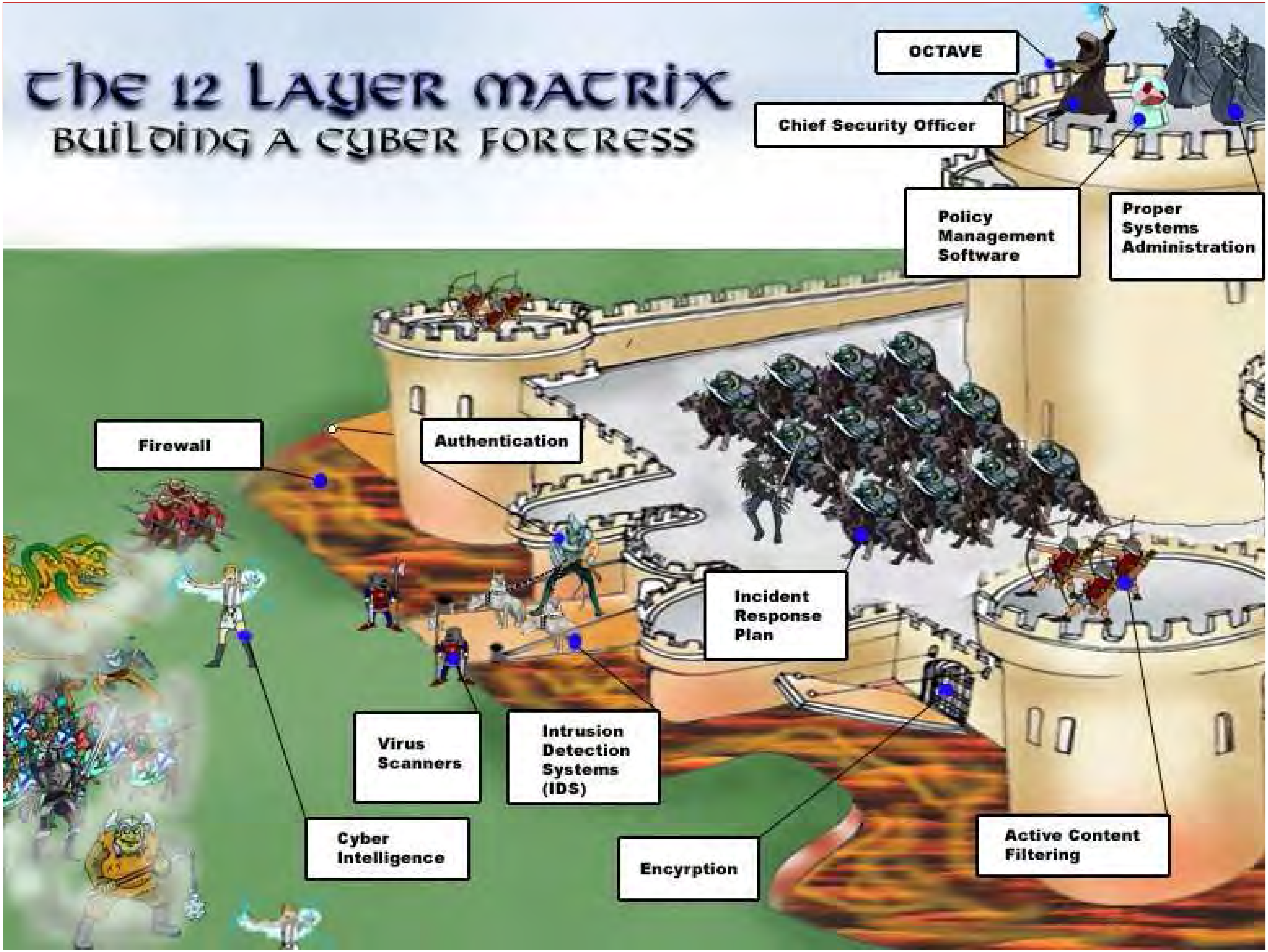
A rootkit is a …

- software tool intended to conceal its presence
- software tool intended to provide concealed access to a system
- set of programs and code that allows a permanent or consistent, undetectable presence on a machine
- *600% increase in the use of rootkits*

- ***Storm worm** utilizes encrypted P2P*
- ***Zeus Trojan** had embedded capabilities*

The 12 Layer Matrix

Building a Cyber Fortress



OCTAVE

Chief Security Officer

Policy Management Software

Proper Systems Administration

Firewall

Authentication

Incident Response Plan

Virus Scanners

Intrusion Detection Systems (IDS)

Cyber Intelligence

Encyrption

Active Content Filtering

Managing the Insider Threat

- Insider threats are real but not just the physical insider but the virtual insider e.g. the compromised device.
- Testing the effectiveness of your internal security polices and procedures and technologies are critical to in order to survive an insider attack.
- Incident response plans should be tested regularly but also should include a penetration test to ascertain where a rogue employee or zombie pc could have transited to within your network as most organizations network topology diagrams are outdated.
- Two-factor authentication, log reviews and least privileged access to systems is key.

Traditional Insider Analysis

- Does a network topology diagram exist, and if so, is it kept up-to-date?
- Have you conducted a business impact analysis? Consequently, do you have an asset based threat profile which would include a definition of potential impact to the enterprise should there be a breach in security (i.e. a loss of confidentiality, integrity or availability)?
- Does a formal computer ethics and hygiene training program exist for all employees?
- Has a formal process been created for reporting negative “anti-enterprise” behavior by employees? Are these reports briefed to management?

Cont.

- Are backdoor audits conducted on employees computers who are disillusioned e.g. *troubled*? Are "sniffers" placed on those machines thereafter?
- Is each user only granted access to data, which the user has a valid *need to know?*
- Are the following logs reviewed regularly as they relate to "troubled" users accounts? * Remote access logs * File access logs * Database logs * System File Change logs * Email logs7.
- Are all activities accountable and traceable to an individual?

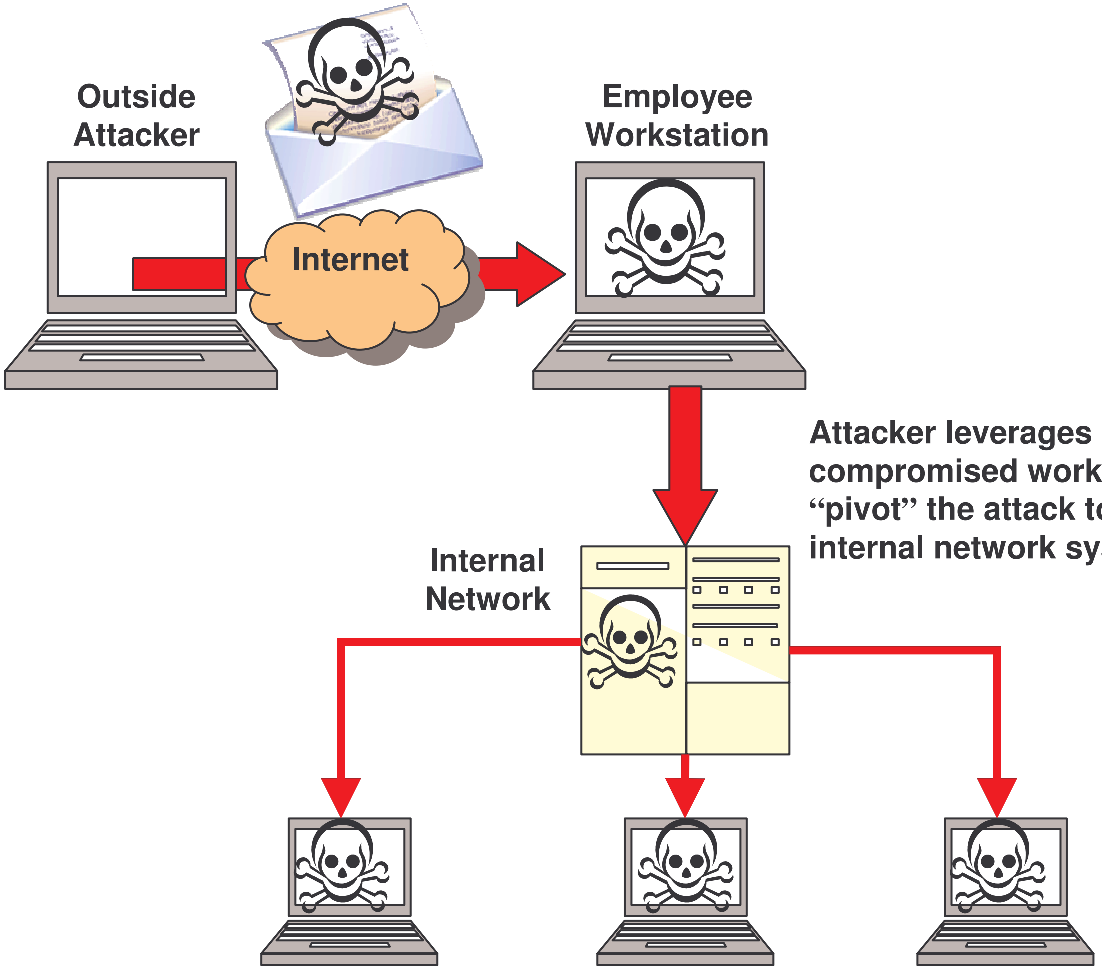
Strategic Third Parties and Island Hopping

- ***Over 30% of breaches were due to strategic partner lapses in security.***
- More electronic records breached in 2008 than the previous four years combined.
- Highly sophisticated attacks account for 17% of breaches, but account for 95% of stolen records.

-Verizon Business, "2009 Data Breach Investigations Report"

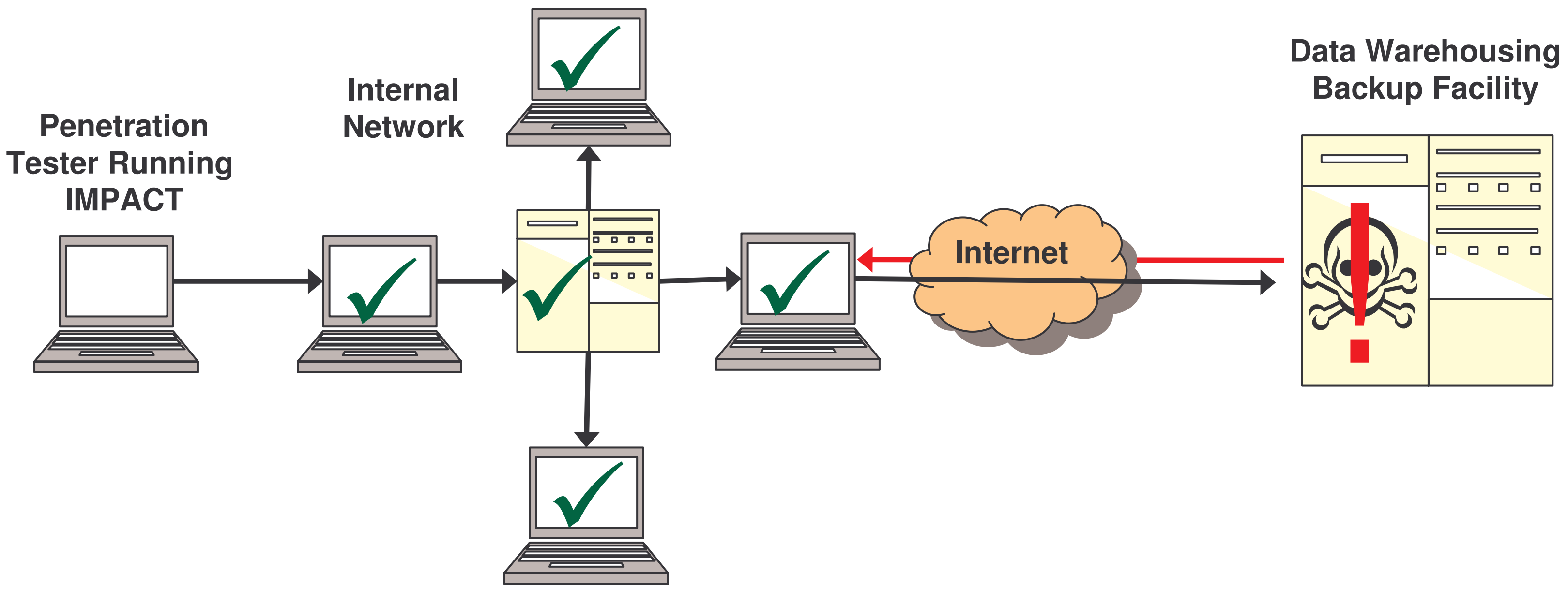
Hosting Companies = Watering Holes

Leapfrogging Perimeters



Attacker leverages compromised workstation to “pivot” the attack to other internal network systems.

Transiting


Penetration Tester Running IMPACT
Internal Network
Internet
Data Warehousing Backup Facility

Managing Risk in Outsourcing

1. Verify that the legal requirements to which the service provider is contractually obligated are compatible with your organization's definition of adequate security (e.g., NIST 800-53).
2. Identify who in the service provider organization is responsible for security oversight (e.g., CSO or CISO). Their Information Systems Security Policy and incident response plan must be reviewed prior to movement of data or provision of service.
3. Confirm that their policies and agreements regarding security breaches include customer notification on a timely basis (within one hour). Maintain the right to test their incident response plan on an annual basis.
4. Confirm that the service provider has adequate backup facilities which are regularly tested for vulnerabilities.
5. On an annual basis, conduct risk assessments of their network security posture, and verify whether they have layered security beyond firewalls, virus scanners and encryption. (NIST 800-53A Appendix G serves as excellent guidance on this matter).

Why Testing is Important

- Hackers attack data where it sits 99.9% of the time: clients, servers and databases
- Nearly 90 percent of 2008 vulnerabilities could be remotely exploited. (IBM/ISS)

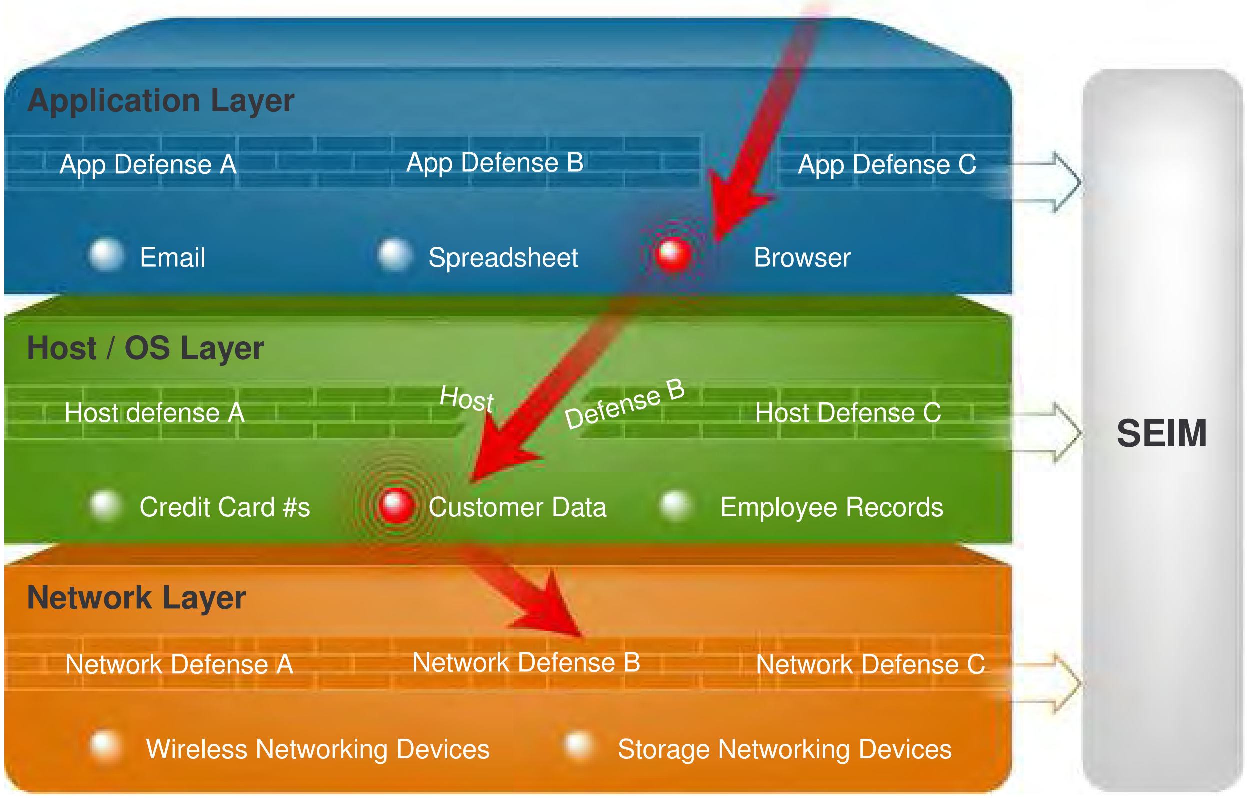
Real-World Attack Behavior

Cybercriminals are still finding their way around, and through, point security defenses.

New attack paths

Point defense weaknesses

Multistaged threats that move across systems and IT layers to threaten critical backend assets



How do you know what's working, what's not, and what to do about it?

Red Teaming--NIST 800-53A Appendix G

- **An effective penetration test goes beyond vulnerability scanning, to offer proof of mission risks and an indicator of how an adversary would to expend resources in order to cause harm to the organization's operations and assets,**

- **An effective penetration test approaches the information system as the adversary would, considering vulnerabilities, incorrect system configurations, trust relationships between organizations, and architectural weaknesses in the environment under test;**

An effective penetration test contains at a minimum:

- A definition of the environment subject to test (e.g., facilities, users, organizational grps et al.)

- A definition of the attack surface to be tested (e.g., servers, desktop systems, wireless networks, web applications, intrusion detection and prevention systems, firewalls, email accounts, user security awareness and training posture, incident response posture, etc.);

- A definition of the threat sources to simulate (e.g., an enumeration of attacker's profiles to be used: internal attacker, casual attacker, single or group of external targeted attackers, criminal organization, etc.);

NIST 800-53A Appendix G Cont.

- **An effective penetration test thoroughly documents all activities performed during the test, including all exploited vulnerabilities, and how the vulnerabilities were combined into attacks;**
- **An effective penetration test produces results indicating a risk level for a given attacker by using the level of effort the team needed to expend in penetrating the information system as an indicator of the penetration resistance of the system;**
- **An effective penetration test validates existing security controls (including risk mitigation mechanisms such as firewalls, intrusion detection and prevention systems);**
- **An effective penetration test provides a verifiable and reproducible log of all the activities performed during the test; and**
- **An effective penetration test provides actionable results with information about possible remediation measures for the successful attacks performed.**

Consensus Audit Guidelines

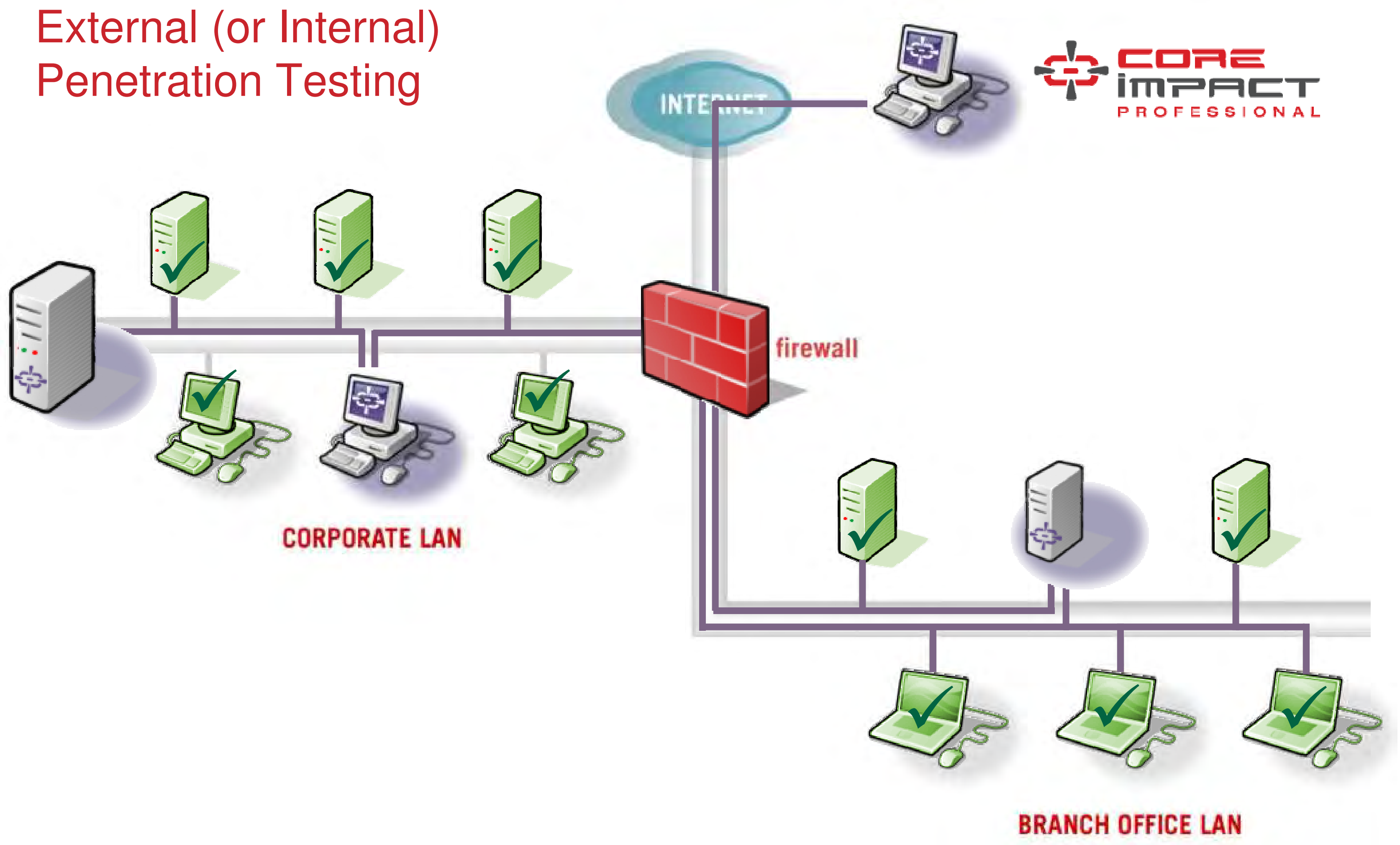
- Critical Control 17: (Excerpt)

---- Penetration Tests and Red Team Exercises: “Organizations should conduct regular penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.”

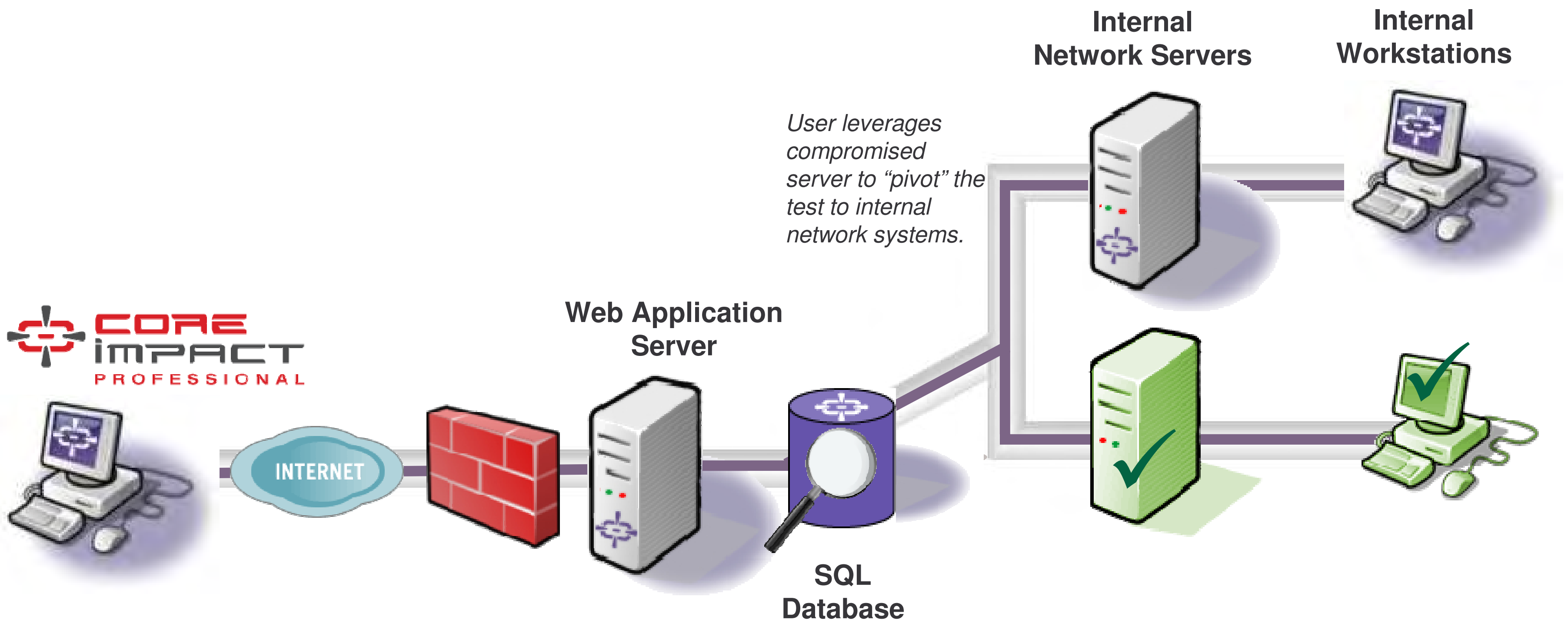
- Critical Control 15: Data Leakage Prevention
- Critical Control 10: Continuous Vulnerability Assessment
- Critical Control 7: Applications Software Security
- Critical Control 5: Boundary Defense
- Critical Control 4: Secure Configurations of Network Devices Such as Firewalls and Routers

CORE IMPACT Pro: Network Security Testing

External (or Internal) Penetration Testing



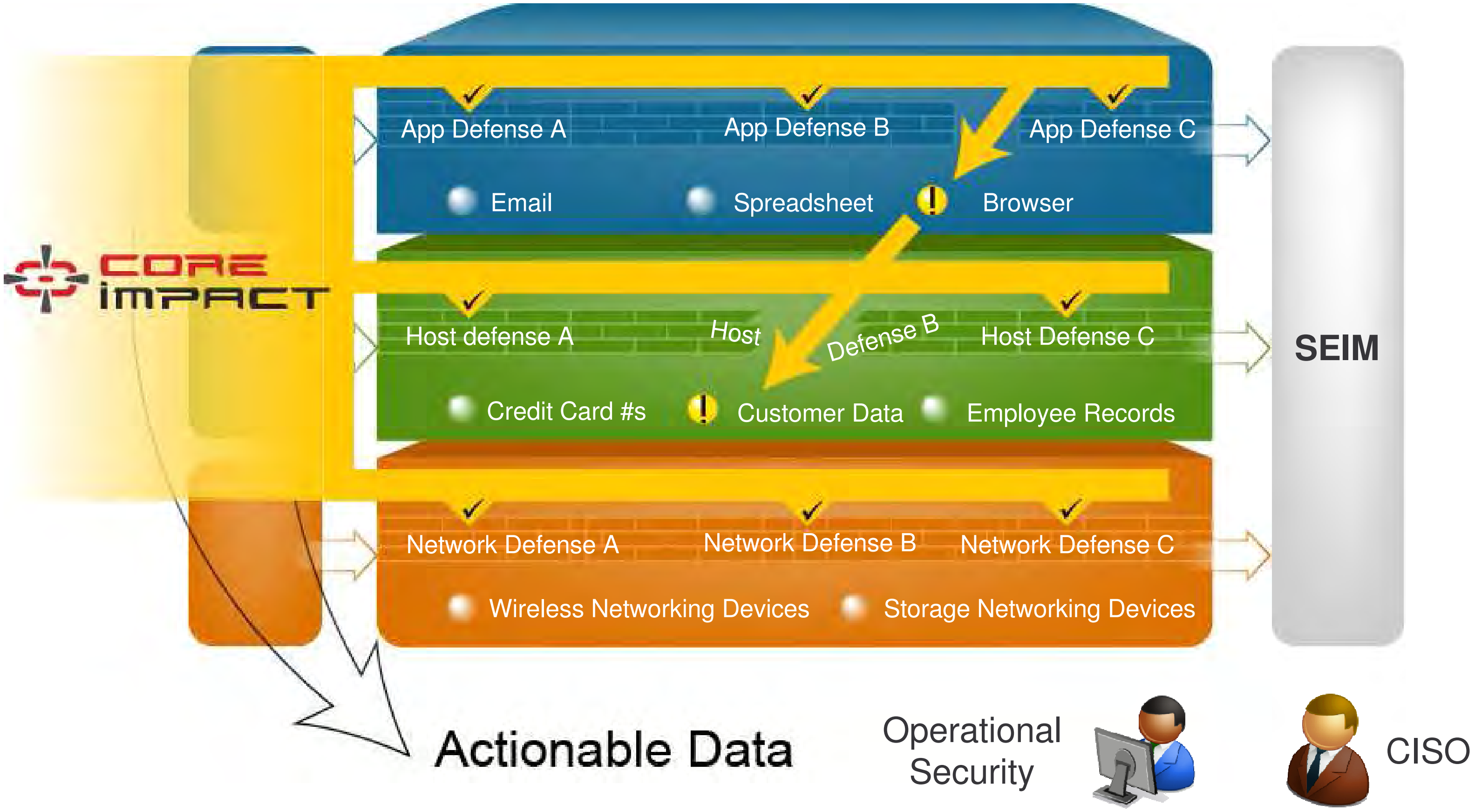
CORE IMPACT Pro: Web App Security Testing



User leverages compromised server to "pivot" the test to internal network systems.

Comprehensive, Real-World Security Testing

By identifying and validating the most critical, exploitable risks, IMPACT enables intelligent vulnerability remediation and helps to prioritize security initiatives.



Critical Security Questions

1. Does the organization have an updated Information Security Policy? Are all users trained and tested per the Acceptable Use Policy?
2. When is the last time the organization conducted a penetration test of its environment? Where is that report and the remediation log?
3. How many third parties e.g. datawarehousers and or web-hosting companies provide services to organization? Has their cyber security posture been audited?
4. Is access to all sensitive systems and computers governed by two factor authentication?
5. Does the organization maintain an cyber incident response plan? If so, when was the last time the plan was tested?
6. If logs are kept, how frequently are they reviewed?
7. Do you run web application scanner to simulate an attack of the website and determine its security?

Mitigating the Clandestine Threat

In 2009, evaluating an organizations:

- Remote connections
- Incident response plans
- Web applications
- Outsourcing arrangements

… will be tantamount preventing the use of their networks by criminals.

The Future of Cyber Attacks

- The biggest threats (in terms of attack attempts & likelihood of success) will be against users' machines or web 2.0+ applications (and a combination of the two, e.g., XSS, etc.).
- The proliferation of mobile devices with powerful computing resources, SaaS and cloud computing, and web applications with distributed architectures using web services from multiple applications service providers may become "game-changing" in the next 5 years.
- At the network level, the migration to IPv6 and the convergence of data and telephony networks with VoIP and related protocols will present the opportunity for more serious threats that what we've seen so far.
- Further down the road, application security will remain an issue, but attacks will move down the stack to embedded OS and virtualization.

For Additional Information …

http://www.coresecurity.com

National Institute of
Standards and Technology
U.S. Department of Commerce

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Draft)

Recommendations of the National Institute of Standards and Technology

Erika McCallister
Tim Grance
Karen Scarfone

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

Acknowledgements

The authors, Erika McCallister, Tim Grance, and Karen Scarfone of the National Institute of Standards and Technology (NIST), wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. Of particular note are the efforts of Joseph Nusbaum of Innovative Analytics & Training, Deanna DiCarlantonio of CUNA Mutual Group, and Michael L. Shapiro and Daniel I. Steinberg of Booz Allen Hamilton, who contributed significant portions to previous versions of the document. The authors would also like to acknowledge Ron Ross, Kelley Dempsey, and Arnold Johnson of NIST; Michael Gerdes, Beth Mallory, and Victoria Thompson of Booz Allen Hamilton; and Julie McEwen and Aaron Powell of MITRE, for their keen and insightful assistance throughout the development of the document. Additional acknowledgements will be added to the final version of the publication.

Note to Reviewers

This publication contains several examples of determining the PII confidentiality impact level to assign to various instances of PII. These examples are intended to illustrate the factors to consider when deciding how to protect the confidentiality of PII, and are not intended to define how certain types of data should always be protected. Every situation has unique characteristics that may affect the assigned impact level and the corresponding protective measures applied to the PII. An organization's legal counsel and privacy officer should be consulted when determining whether there are legal obligations to protect the confidentiality of PII. The authors welcome feedback on the examples, such as different opinions on the appropriate impact levels and suggestions for additional examples that would be helpful to readers. Finally, the authors are also seeking suggestions for feasible technical solutions for logging and verifying sensitive database extracts, as described in Appendix E. NIST thanks the reviewers in advance for sharing their expertise and valuable time to perform this public service.

Table of Contents

Appendices

Executive Summary

Breaches of personally identifiable information (PII) have increased dramatically over the past few years and have resulted in the loss of millions of records.[1] Breaches of PII are hazardous to both individuals and organizations. Individual harms may include identity theft, embarrassment, or blackmail. Organizational harms may include a loss of public trust, legal liability, or high costs to handle the breach. To appropriately protect the confidentiality of PII, organizations should use a risk-based approach; as McGeorge Bundy[2] once stated, "If we guard our toothbrushes and diamonds with equal zeal, we will lose fewer toothbrushes and more diamonds." This document provides guidelines for a risk-based approach to protecting the confidentiality[3] of PII.

The recommendations in this document are intended primarily for U.S. Federal government agencies and those who conduct business on behalf of the agencies,[4] but other organizations may find portions of the publication useful. Each organization may be subject to a different combination of laws, regulations, and other mandates related to protecting PII, so an organization's legal counsel and privacy officer should be consulted to determine the current obligations for PII protection. For example, the Office of Management and Budget (OMB) has issued several memoranda with requirements for how Federal agencies must handle and protect PII.

To effectively protect PII, organizations should implement the following recommendations.

Organizations should identify all PII residing in their environment.

An organization cannot properly protect PII it does not know about. This document uses the broad definition of PII from OMB Memorandum 07-16[5] to identify as many potential sources of risks related to PII as possible. OMB defined PII as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." Examples of PII include, but are not limited to:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), fingerprints, handwriting, or other biometric image or template data (e.g., retina scans, voice signature, facial geometry).

[1] Government Accountability Office (GAO) Report 08-343, *Protecting Personally Identifiable Information*, January 2008, http://www.gao.gov/new.items/d08343.pdf

[2] Congressional testimony as quoted by the New York Times, March 5, 1989. McGeorge Bundy was the U.S. National Security Advisor to Presidents Kennedy and Johnson (1961-1966). http://query.nytimes.com/gst/fullpage.html?res=950DE2D6123AF936A35750C0A96F948260

[3] For the purposes of this document, confidentiality is defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information." 44 U.S.C. § 3542. http://uscode.house.gov/download/pls/44C35.txt.

[4] For the purposes of this publication, both are referred to as "organizations".

[5] OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

Organizations should categorize their PII by the PII confidentiality impact level.

All PII is not created equal. PII should be evaluated to determine its PII confidentiality impact level so that appropriate safeguards can be applied to the PII. The PII confidentiality impact level—*low, moderate, or high*—indicates the potential harm that could result to the subject individuals and/or the organization if the PII were inappropriately accessed, used, or disclosed. This document provides a list of factors an organization should consider when determining the PII confidentiality impact level. Each organization should decide which factors it will use for determining impact levels and then create and implement the appropriate policy, procedures, and controls. The following are examples of factors:

- **Distinguishability.** Organizations should evaluate how easily the PII can be used to distinguish particular individuals. For example, an SSN uniquely identifies an individual, whereas a telephone area code could map to many people.

- **Aggregation and Data Field Sensitivity.** Organizations should evaluate the sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields when combined. For example, an individual's SSN or financial account number is generally more sensitive than an individual's phone number or zip code. Similarly, the combination of an individual's name and financial account number is more sensitive than the individual's name alone.

- **Context of Use.** Organizations should evaluate the context of use, which is the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated. The context of use may cause identical PII data elements to be assigned different PII confidentiality impact levels based on their use. For example, suppose that an organization has two lists that contain the same PII data fields (e.g., name, address, phone number). The first list is people who subscribe to a general-interest newsletter produced by the organization, and the second list is people who work undercover in law enforcement. The potential impacts to the affected individuals and to the organization are significantly different for each list.

- **Obligations to Protect Confidentiality.** An organization that is subject to any obligations to protect PII should consider such obligations when determining the PII confidentiality impact level. Obligations to protect generally include laws, regulations, or other mandates (e.g., Privacy Act, OMB guidance). For example, some Federal agencies, such as the Census Bureau and the Internal Revenue Service (IRS), are subject to specific legal obligations to protect certain types of PII.[6]

- **Access to and Location of PII.** Organizations may choose to take into consideration the nature of authorized access to and the location of the PII. When PII is accessed more often or by more people and systems, or the PII is regularly transmitted or transported offsite, then there are more opportunities to compromise the confidentiality of the PII.

Organizations should apply the appropriate safeguards for PII based on the PII confidentiality impact level.

Not all PII should be protected in the same way. Organizations should apply appropriate safeguards to protect the confidentiality of the PII based on the PII confidentiality impact level. Some PII does not need to have its confidentiality protected, such as information that the organization has permission or authority to release publicly (e.g., an organization's public phone directory). NIST recommends using

[6] The Census Bureau has a special obligation to protect based on provisions of Title 13 of the U.S. Code, and IRS has a special obligation to protect based on Title 26 of the U.S. Code. There are more agency-specific obligations to protect PII, and an organization's legal counsel and privacy officer should be consulted.

general protection measures, privacy-specific protection measures, and security controls[7] used for other types of information, such as:

- **Creating Policies and Procedures.** Organizations should develop comprehensive policies and procedures for protecting the confidentiality of PII.
- **Conducting Training.** Organizations should reduce the possibility that PII will be accessed, used, or disclosed inappropriately by requiring that all individuals receive appropriate training before being granted access to organization information systems.
- **De-Identifying PII.** Organizations can de-identify records by removing enough PII such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. De-identified records can be used when full data records are not necessary, such as for examinations of correlations and trends.
- **Using Access Enforcement.** Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists).
- **Implementing Access Control for Mobile Devices.** Organizations can prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities). Organizations may choose to forbid all telework and remote access involving higher-impact instances of PII so that the information will not leave the organization's physical boundaries through telework activities.
- **Providing Transmission Confidentiality.** Organizations can protect the confidentiality of transmitted PII. This is most often accomplished by encrypting the communications or by encrypting the information before it is transmitted.
- **Auditing Events.** Organizations can monitor events that affect the confidentiality of PII, such as inappropriate access to PII.

Organizations should minimize the collection and retention of PII to what is strictly necessary to accomplish their business purpose and mission.

The likelihood of harm caused by a breach of PII is greatly reduced if an organization minimizes the amount of PII it collects and stores. Organizations should limit PII collection and retention to the least amount necessary to conduct their business purpose and mission. For example, an organization should only request PII on a new form if the PII is absolutely necessary. Also, an organization should regularly review its holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting the organization's business purpose and mission. For example, organizations could have an annual PII purging awareness day.[8]

OMB M-07-16 specifically requires agencies to:

- Review current holdings of PII and ensure they are accurate, relevant, timely, and complete
- Reduce PII holdings to minimum necessary for proper performance of agency functions
- Develop a schedule for periodic review of PII holdings

[7] This document provides some selected security control examples from NIST SP 800-53.

[8] Disposal of PII should be conducted in accordance with the retention schedules approved by the National Archives and Records Administration (NARA).

- Establish a plan to eliminate the unnecessary collection and use of SSNs.

Organizations should develop an incident response plan to handle breaches of PII.

Breaches of PII are hazardous to both individuals and organizations. Harm to individuals and organizations can be contained and minimized through the development of effective incident response plans for PII breaches. Organizations should develop plans[9] that include elements such as determining when and how individuals should be notified, when and if a breach should be reported publicly, and whether to provide remedial services, such as credit monitoring, to affected individuals. Organizations should integrate these additional policies into their existing incident handling policies.

Organizations should encourage close coordination among their privacy officers, chief information officers, information security officers, and legal counsel[10] when addressing issues related to PII.

Protecting the confidentiality of PII requires knowledge of information systems, information security, privacy, and legal requirements. Decisions regarding the applicability of a particular law, regulation, or other mandate should be made in consultation with an organization's legal counsel and privacy officer because relevant laws, regulations, and other mandates are often complex and change over time. Additionally, new policies often require the implementation of technical security controls to enforce the policies. Close coordination of the relevant experts helps to prevent PII breaches by ensuring proper interpretation and implementation of requirements.

[9] OMB M-07-16 requires agencies to develop and implement breach notification policies.

[10] Some organizations are structured differently and have different names for roles. These roles are examples, used for illustrative purposes.

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies, also referred to as organizations in the guide. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

The purpose of this document is to assist Federal agencies in protecting the confidentiality of a specific category of data commonly known as personally identifiable information (PII). PII should be protected from inappropriate access, use, and disclosure. This document provides practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII. The document also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for breaches involving PII. Organizations are encouraged to tailor the recommendations to meet their specific requirements.

1.3 Audience

The primary audience for this document is the individuals who apply policies and procedures for protecting the confidentiality of PII on Federal information systems, as well as technical and non-technical personnel involved with implementing system-level changes concerning PII protection methods. Individuals in many roles should find this document useful, including chief privacy officers and other privacy officers, privacy advocates, privacy support staff, compliance officers, system administrators, chief information system security officers, information system security officers, information security support staff, computer security incident response teams, and chief information officers.

1.4 Document Structure

The remainder of this document is organized into the following sections:

- Section 2 provides an introduction to PII and lists some basic requirements involving the collection and handling of PII.

- Section 3 describes factors for determining the potential impact of inappropriate access, use, and disclosure of PII.
- Section 4 presents several methods for protecting the confidentiality of PII that can be implemented to reduce PII exposure and risk.
- Section 5 provides recommendations for developing an incident response plan for breaches involving PII and integrating the plan into an organization's existing incident response plan.

The following appendices are also included for additional information:

- Appendix A provides samples of PII-related scenarios and questions that can be adapted for an organization's exercises.
- Appendix B presents frequently asked questions (FAQ) related to protecting the confidentiality of PII.
- Appendix C contains definitions of common general terms related to private information.
- Appendix D provides additional information about the Fair Information Practices that may be helpful in understanding the framework underlying most privacy laws.
- Appendix E contains a FAQ pertaining to logging and verifying sensitive database extracts.
- Appendix F provides a glossary of selected terms from the publication.
- Appendix G contains a list of acronyms and abbreviations used within the publication.
- Appendix H presents a list of resources that may be helpful to individuals in gaining a better understanding of PII, PII protection, and other related topics.

2. Introduction to PII

One of the most broadly used terms to describe personal information about individuals is PII. Examples of PII range from an individual's name or email address to an individual's financial and medical records or criminal history. Unauthorized access, use, or disclosure of PII can seriously impact both individuals, by contributing to identity theft, and the organization, by reducing public trust in the organization. In many cases, it may not be clear to the professionals responsible for protecting information which instances of PII need additional confidentiality protection and at what level. This section explains how to identify and locate PII[11] maintained within an organization's environment and/or under its control, and it provides an introduction to the Fair Information Practices. Sections 3 and 4 discuss factors for assigning PII impact levels and selecting protection measures, respectively. Section 5 discusses incident response for breaches involving PII.

2.1 Identifying PII

This publication uses the definition of PII from OMB Memorandum 07-16,[12] which is "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

To distinguish an individual[13] is to identify an individual. Some examples of information that could distinguish an individual include, but are not limited to, name, passport number, social security number, or biometric image and template. In contrast, a list containing only credit scores does not have sufficient information to distinguish a specific individual.

Information elements that are linked or linkable are not sufficient to distinguish an individual when considered separately, but which could distinguish individuals when combined with a secondary information source. For example, suppose that two databases contain different PII elements and also share some common PII elements. An individual with access to both databases may be able to link together information from the two databases and distinguish individuals. If the secondary information source is present on the same system or a closely-related system, then the data is considered *linked*. If the secondary source is available to the general public or can be obtained, such as from an unrelated system within the organization, then the data is considered *linkable*. Linked data is often de-identified in some way (as described in Section 4), and information that makes re-identification possible is available to some system users. Linkable data is also often de-identified, but the remaining data can be analyzed against other data sources, such as telephone directories and other sources available to large communities of people, to distinguish individuals.

Organizations should use a variety of methods to identify all PII residing within their organization or under the control of their organization through a third party (e.g., a system being developed and tested by a contractor). Privacy threshold analyses (PTAs), also referred to as initial privacy assessments (IPAs), are often used to identify PII.[14] Some organizations require a PTA to be completed before the

[11] Even if an organization determines that information is not PII, the organization should still consider whether the information is sensitive or has organizational or individual risks associated with it, and determine the appropriate protections.

[12] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

[13] The terms "individual" and "individual's identity" are used interchangeably throughout this document. For additional information about the term *individual*, see Appendix B.

[14] For example PTA/IPA templates, see: http://www.usdoj.gov/opcl/initial-privacy-assessment.pdf or http://www.dod.mil/pubs/foi/privacy/DHS_PTA_Template.pdf.

development or acquisition of a new information system and when a substantial change is made to an existing information system. PTAs are used to determine if a system contains PII, whether a Privacy Impact Assessment is required, whether a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. PTAs should be submitted to an organization's privacy office for review and approval. PTAs are often comprised of simple questionnaires that are completed by the system owner. PTAs are useful in initiating the communication and collaboration for each system between the privacy officer, the information security officer, and the information officer. Other examples of methods to identify PII include reviewing system documentation, conducting interviews, conducting data calls, or checking with system owners.

2.2 Examples of PII Data

The following list contains examples of information that may be considered PII.[15]

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as SSN, passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number[16]
- Address information, such as street address or email address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scans, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration or identification number, and title numbers and related information
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, or employment, medical, education, or financial information).

2.3 PII and Fair Information Practices

The protection of PII and the overall privacy of records are concerns both for individuals whose personal records are at stake and for organizations that may be liable or have their reputations damaged should such PII be inappropriately accessed, used, or disclosed. Treatment of PII is distinct from other types of data because it needs to be not only protected, but also collected, maintained, and disseminated in accordance with Federal law.[17] The Privacy Act, as well as other privacy laws, is based on the widely-recognized Fair Information Practices, also called Privacy Principles. There are five core Fair

[15] As discussed in Section 3, the risk posed by these examples and the appropriate protections needed for each vary on a case-by-case basis.

[16] Partial identifiers, such as the first few digits or the last few digits of SSNs, are also often considered PII because they are still nearly unique identifiers and are linked or linkable to a specific individual.

[17] This document focuses on protecting the confidentiality of PII. Protecting the privacy of PII is a broader subject, and information about the Fair Information Practices is provided to increase reader awareness.

Information Practices[18] that are based on the common elements, or privacy principles, of several international reports and guidelines. These core practices are as follows:

- **Notice/Awareness**—Individuals should be given notice of an organization's information practices before any personal information is collected from them.
- **Choice/Consent**—Individuals should be given a choice about how information about them is used.
- **Access/Participation**—Individuals should have the right to access information about them and request correction to ensure the information is accurate and complete.
- **Integrity/Security**—Data collectors should ensure that information is protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- **Enforcement/Redress**—Data collectors should be held accountable for complying with measures that give effect to the practices stated above.

For more information on the Fair Information Practices, including a summary of variations of the Fair Information Practices, see Appendix D.

[18] See: http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

3. PII Confidentiality Impact Levels

This publication focuses on protecting PII from losses of confidentiality. The security objective of confidentiality is defined by law as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[19] The security objectives of integrity and availability may also be important for PII, and organizations should use the NIST Risk Management Framework to determine the appropriate integrity and availability impact levels. Organizations may also need to consider PII-specific enhancements to the integrity or availability impact levels. For example, malicious alterations of medical test results could endanger individuals' lives.

The confidentiality of PII should be protected based on its risk level. This section outlines factors for determining the PII confidentiality impact level for a particular instance of PII, which is distinct from the confidentiality impact level described in Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.*[20] The PII confidentiality impact level takes into account additional PII considerations and should be used to determine if additional protections should be implemented. The PII confidentiality impact level—*low, moderate, or high*—indicates the potential harm that could result to the subject individuals and/or the organization if the PII were inappropriately accessed, used, or disclosed. Once the PII confidentiality impact level is selected, it should be used to supplement the provisional confidentiality impact level, which is determined from information and system categorization processes outlined in FIPS 199 and NIST Special Publication (SP) 800-60, *Volumes 1 and 2: Guide for Mapping Types of Information and Information Systems to Security Categories.*[21]

Some PII does not need to have its confidentiality protected, such as information that the organization has permission or authority to release publicly (e.g., an organization publishing a phone directory of employees' names and work phone numbers so that members of the public can contact them directly). In this case, the PII confidentiality impact level would be *not applicable* and would not be used to supplement a system's provisional confidentiality impact level. PII that does not require confidentiality protection may still require other security controls to protect the integrity and the availability of the information, and the organization should provide appropriate security controls based on the assigned FIPS 199 impact levels.

3.1 Impact Level Definitions

The harm caused from of a loss of confidentiality should be considered when attempting to determine which PII confidentiality impact level corresponds to a specific set of PII data. *Harm* for the purposes of this document, includes any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII. Harm to an individual includes any negative or unwanted effects (i.e., that may be socially, physically, or financially damaging). Examples of types of harm to individuals include, but are not limited to, the potential for blackmail, identity theft, physical harm, discrimination, or emotional distress. Organizations may also experience harm as a result of a loss of confidentiality of PII maintained by the organization—including but not limited to administrative burden, financial losses, loss of public reputation and public confidence, and civil liability.

[19] 44 U.S.C. § 3542, http://uscode.house.gov/download/pls/44C35.txt

[20] http://csrc.nist.gov/publications/PubsFIPS.html

[21] http://csrc.nist.gov/publications/PubsSPs.html

The following describe the three impact levels—low, moderate, and high—defined in FIPS 199, which are based on the potential impact of a security breach involving a particular system:[22]

> "The potential impact is **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
>
> The potential impact is **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
>
> The potential impact is **HIGH** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries."

Harm to individuals as described in these impact levels is easier to understand with examples. A breach of the confidentiality of PII at the low impact level would not cause harm greater than inconvenience, such as changing a telephone number. The types of harm that could be caused by a breach of PII at the moderate impact level include financial loss due to identity theft or denial of benefits, public humiliation, discrimination, and the potential for blackmail. Harm at the high impact level involves serious physical, social, or financial harm, resulting in potential loss of life or inappropriate physical detention.

3.2 Factors for Determining PII Confidentiality Impact Levels

Determining the PII confidentiality impact level should take into account relevant factors. Several important factors that organizations should consider are described below. It is important to note that relevant factors should be considered together; one factor by itself might indicate a low impact level, but another factor might indicate a high impact level, and thus override the first factor. Also, the impact levels suggested for these factors are for illustrative purposes; each instance of PII is different, and each organization has a unique set of requirements and a different mission. Therefore, organizations should determine which factors, including organization-specific factors, they should use for determining PII confidentiality impact levels and should create and implement policy and procedures that support these determinations.

[22] This document pertains only to the confidentiality impact and does not address integrity or availability.

3.2.1 Distinguishability

Organizations should evaluate how easily the PII can be used to distinguish particular individuals. For example, PII data composed of individuals' names, fingerprints, and SSNs uniquely identify individuals, whereas PII data composed of individuals' phone numbers only would require the use of additional data sources, such as phone directories, and would only allow some unique individuals to be identified (for example, unique identification might not be possible if multiple individuals share a phone or if a phone number is unlisted). PII data composed of only individuals' area codes and gender would not allow any unique individuals to be identified.[23] PII that is easily distinguishable may merit a higher impact level than PII that cannot be used to distinguish individuals without unusually extensive efforts.

Organizations may also choose to consider how many individuals can be distinguished from the PII data. Breaches of 25 records and 25 million records may have different impacts, not only in terms of the collective harm to individuals but also in terms of harm to the organization's reputation and the cost to the organization in addressing the breach. For this reason, organizations may choose to set a higher impact level for particularly large PII data sets than would otherwise be set. However, organizations should not set a lower impact level for a PII data set simply because it contains a small number of records.

3.2.2 Aggregation and Data Field Sensitivity

Organizations should evaluate the sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields together. For example, an individual's SSN or financial account number is generally more sensitive than an individual's phone number or zip code, and the combination of an individual's name and SSN is less sensitive than the combination of an individual's name, SSN, date of birth, mother's maiden name, and credit card number. Organizations often require the PII confidentiality impact level to be set to at least moderate if a certain sensitive data field, such as SSN, is present. Organizations may also consider certain combinations of PII data fields to be more sensitive, such as name and credit card number, than each data field would be considered without the existence of the others.

3.2.3 Context of Use

Context of use is defined as the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated, as well as how that PII is used or could potentially be used. Examples of context include, but are not limited to, statistical analysis, determining eligibility for benefits, administration of benefits, research, tax administration, or law enforcement. Organizations should assess the context of use because it is important to understanding how the disclosure of data elements can potentially harm individuals and the organization. Organizations should consider what harm is likely to be caused if the PII is disclosed (either intentionally or accidentally) or if the mere fact that the PII is being collected or used is disclosed could cause harm to the organization or individual. For example, law enforcement investigations could be compromised if the mere fact that information is being collected about a particular individual is disclosed.

The context of use may cause multiple instances of the same types of PII data to be assigned different PII confidentiality impact levels. For example, suppose that an organization has three lists that contain the same PII data fields (e.g., name, address, phone number). The first list is people who subscribe to a general-interest newsletter produced by the organization. The second list is people who have filed for retirement benefits, and the third list is individuals who work undercover in law enforcement. The potential impacts to the affected individuals and to the organization are significantly different for each of

[23] Section 4.2 discusses how organizations can reduce the need to protect PII by removing PII from records.

the three lists. Based on context of use only, the three lists are likely to merit impact levels of low, moderate, and high, respectively.

Examples of topics that are relevant to context of use as a factor for determining PII confidentiality impact level are abortion; alcohol, drug, or other addictive products; illegal conduct; illegal immigration status; information damaging to financial standing, employability, or reputation; information leading to social stigmatization or discrimination; politics; psychological well-being or mental health; religion; same-sex partners; sexual behavior; sexual orientation; taxes; and other information due to specific cultural or other factors.[24]

3.2.4 Obligation to Protect Confidentiality

An organization that is subject to any obligations to protect PII should consider such obligations when determining the PII confidentiality impact level. Many organizations are subject to laws, regulations, or other mandates[25] governing the obligation to protect personal information,[26] such as the Privacy Act of 1974, OMB memoranda, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Additionally, some Federal agencies, such as the Census Bureau and the Internal Revenue Service (IRS), are subject to additional specific legal obligations to protect certain types of PII.[27] Some organizations are also subject to specific legal requirements based on their role. For example, organizations acting as financial institutions by engaging in financial activities are subject to the Gramm-Leach-Bliley Act (GLBA).[28] Also, some agencies that collect PII for statistical purposes are subject to the strict confidentiality requirements of the Confidential Information Protection and Statistical Efficiency Act (CIPSEA).[29] Violations of many of these laws can result in civil or criminal penalties. Organizations may also be obliged to protect PII by their own policies, standards, or management directives.

For example, a database with PII for beneficiaries of government services that retrieves information by SSN would be considered a System of Records under the Privacy Act of 1974, and the organization would be required to provide appropriate administrative, technical, and physical safeguards for the database. Decisions regarding the applicability of a particular law, regulation, or other mandate should be made in consultation with an organization's legal counsel and privacy officer because relevant laws, regulations, and other mandates are often complex and change over time.

3.2.5 Access to and Location of the PII

Organizations may choose to take into consideration the nature of authorized access to the PII. When PII is accessed more often or by more people and systems, there are more opportunities for the PII's confidentiality to be compromised. Another element is the scope of access to the PII, such as whether the PII needs to be accessed from teleworkers' systems and other systems outside the direct control of the organization. These considerations could cause an organization to assign a higher impact level to widely-

[24] See *Guide to U.S. Census Bureau Data Stewardship/Privacy Impact Assessments (DS/PIAs),* http://www.census.gov/po/pia/Guide_to_PIAs.doc

[25] See Appendix H for additional resources.

[26] Personal information is defined in different ways by different laws, regulations, and other mandates. Many of these definitions are not interchangeable. Therefore, it is important to use each specific definition to determine if an obligation to protect exists for each type of personal information. See Appendix C for a listing of common definitions of personal information.

[27] The Census Bureau has a special obligation to protect based on provisions of Title 13 of the U.S. Code, and IRS has a special obligation to protect based on Title 26 of the U.S. Code. There are more agency-specific obligations to protect PII, and an organization's legal counsel and privacy officer should be consulted.

[28] For additional information, see GLBA, 15 U.S.C. § 6801 et seq.

[29] CIPSEA is Title 5 of the E-Government Act of 2002, Pub.L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101 et seq. CIPSEA covers all types of data collected for statistical purposes, not just PII. For additional information, see the OMB Implementation Guidance for CIPSEA, http://www.whitehouse.gov/omb/fedreg/2007/061507_cipsea_guidance.pdf.

accessed PII than would otherwise be assigned to help mitigate the increased risk caused by the nature of the access.

Additionally, organizations may choose to consider whether PII that is stored or regularly transported off-site by employees should be assigned a higher PII confidentiality impact level. For example, surveyors, researchers, and other field employees often need to store PII on laptops or removable media as part of their jobs. PII located offsite is more vulnerable to unauthorized access or disclosure because it is more likely to be lost or stolen than PII stored within the physical boundaries of the organization.

3.3 PII Confidentiality Impact Level Examples

The following are examples of how an organization might assign PII confidentiality impact levels to specific instances of PII. The examples are intended to help organizations better understand the process of considering the various impact level factors, and they are not a substitute for organizations analyzing their own situations. Certain circumstances within any organization or specific system, such as the context of use or obligation to protect, may cause different outcomes.

Obligation to protect is a particularly important factor that should be determined early in the categorization process. Since obligation to protect confidentiality should always be made in consultation with an organization’s legal counsel and privacy officer, it is not addressed in the following examples.

3.3.1 Example 1: Incident Response Roster

An organization maintains a roster (in both electronic and paper formats) of its computer incident response team members. In the event that an IT staff member detects any kind of security breach, standard practice requires that the staff member contact the appropriate people listed on the roster. Because this team may need to coordinate closely in the event of an incident, the contact information includes names, professional titles, office and work cell phone numbers, and work email addresses. The organization makes the same types of contact information available to the public for all of its employees on its main Web site.

Distinguishability: The information directly identifies a small number of individuals (fewer than 20).

Aggregation and data field sensitivity: Although the roster is intended to be made available only to the team members, the individuals’ information included in the roster is already available to the public on the organization’s Web site.

Context of use: The release of the individuals’ names and contact information would not likely cause harm to the individuals, and disclosure of the fact that the organization has collected or used this information is also unlikely to cause harm.

Access to and location of the PII: The information is accessed by IT staff members that detect security breaches, as well as the team members themselves. The PII needs to be readily available to teleworkers and to on-call IT staff members so that incident responses can be initiated quickly.

Taking into account these factors, the organization determines that unauthorized access to the roster would likely cause little or no harm, and it chooses to assign the PII confidentiality impact level of *low*.

3.3.2 Example 2: Intranet Activity Tracking

An organization maintains a Web use audit log for an intranet Web site accessed by employees. The Web use audit log contains the following:

- The user's IP address
- The Uniform Resource Locator (URL) of the Web site the user was viewing immediately before coming to this Web site (i.e., referring URL)
- The date and time the user accessed the Web site
- The amount of time the user spent at the Web site
- The web pages or topics accessed within the organization's Web site (e.g., organization security policy).

Distinguishability: By itself, the log does not contain any distinguishable data. However, the organization has another system with a log that contains domain login information records, which include user IDs and corresponding IP addresses. Administrators that can access both systems and their logs and took the time to correlate information between the logs could distinguish individuals. Potentially, information could be gathered on the actions of most of the organization's users involving Web access to intranet resources. The organization has a small number of administrators that have access to both systems and both logs.

Aggregation and data field sensitivity: The information on which internal Web pages and topics were accessed could potentially cause some embarrassment if the pages involved certain human resources-related subjects, such as a user searching for information on substance abuse programs. However, since the logging is limited to use of intranet-housed information, the amount of potentially embarrassing information is minimal.

Context of use: The release of the information would be unlikely to cause harm, other than potentially embarrassing a small number of users if their identities could be distinguished. The fact that the logging is occurring is generally known and assumed and would not cause harm.

Access to and location of the PII: The log is accessed by a small number of system administrators when troubleshooting operational problems and also occasionally by a small number of incident response personnel when investigating internal incidents. All access to the log occurs only from the organization's own systems.

Taking into account these factors, the organization determines that a breach of the log's confidentiality would likely cause little or no harm, and it chooses to assign the PII confidentiality impact level of *low*.

3.3.3 Example 3: Fraud, Waste, and Abuse Reporting Application

A database contains Web form submissions by individuals claiming possible fraud, waste, or abuse of organizational resources and authority. Some of the submissions include serious allegations, such as accusing individuals of accepting bribes or accusing individuals of not enforcing safety regulations. The submission of contact information is not prohibited, and individuals sometimes enter their personal information in the form's narrative text field. The Web site is hosted by a server that logs IP address, referring Web site information, and time spent on the Web site.

Distinguishability: By default, the database does not request distinguishable data, but a significant percentage of users choose to provide distinguishable information. A recent estimate indicated that the database has approximately 30 records with distinguishable information out of nearly 1000 total records. The Web log does not contain any distinguishable information, nor could it be readily linked with the database or other sources to identify specific individuals.

Aggregation and data field sensitivity: The database's narrative text field contains user-supplied text and frequently includes information such as name, mailing address, email address, and phone numbers. The organization does not know how sensitive this information might be to the individuals, such as unlisted phone numbers or email addresses used for limited private communications.

Context of use: Because of the nature of the submissions—reporting claims of fraud, waste, or abuse—the disclosure of individuals' identities would likely cause some of the individuals making the claims to fear retribution by management and peers. The ensuing harm could include blackmail, severe emotional distress, loss of employment, and physical harm. A breach would also undermine trust in the organization by both the individuals making the claims and the public.

Access to and location of the PII: The database is only accessed by a few people who investigate fraud, waste, and abuse claims. All access to the database occurs only from the organization's own systems.

Taking into account these factors, the organization determines that a breach of the database's confidentiality would likely cause catastrophic harm to some of the individuals and chooses to assign the PII confidentiality impact level of *high*.

4. PII Confidentiality Protection Measures

PII should be protected through a combination of measures, including general protection measures, privacy-specific protection measures, and security controls. Organizations should use a risk-based approach for protecting the confidentiality of PII. The PII protection measures provided in this section are complementary to other general protection measures for data and may be used as one part of an organization's comprehensive approach to protecting the confidentiality of PII.

4.1 General Protection Measures

This section describes two types of general PII protection: policy and procedure creation; and education, training, and awareness.

4.1.1 Policy and Procedure Creation

Organizations should develop comprehensive policies and procedures for handling PII at the organization level, the program or component level, and occasionally the system level.[30] Some types of policies include foundational privacy principles, privacy rules of behavior, policies that implement laws and other mandates, and system-level policies. The organizational privacy principles act as the foundation upon which the overall privacy program is built and reflect the organization's privacy objectives. Foundational privacy principles may also be used as a guide against which to develop additional policies and procedures. Privacy rules of behavior policies provide guidance on the proper handing of PII, as well as the consequences for failure to comply with the policy. Some policies provide guidance on implementing laws and OMB guidance in an organization's environment based upon the organization's authorized business purposes and mission. Organizations should consider developing privacy policies and associated procedures for the following topics:

- Development of Privacy Impact Assessments (PIAs) and coordination with System of Records Notices (SORNs)
- Access rules for PII within a system
- PII retention schedules and procedures
- Redress
- Individual consent
- Data sharing agreements
- PII incident response and data breach notification
- Privacy in the System Development Life Cycle Process
- Limitation of collection, disclosure, sharing, and use of PII

[30] There are laws and OMB guidance that provide agency requirements for policy development. For example, OMB Memorandum 05-08 requires that a "senior agency official must…have a central policy-making role in the agency's development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy issues…" Additionally, the Privacy Act requires agencies to "establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of…" the Privacy Act "including any other rules and procedures adopted…and the penalties for noncompliance."

- Consequences for failure to follow privacy rules of behavior.

If the organization permits access to or transfer of PII through interconnected systems external to the organization or shares PII through other means, the organization should implement the appropriate documented agreements for roles and responsibilities, restrictions on further sharing of the information, requirements for notification to each party in the case of a breach, minimum security controls, and other relevant factors. Also, Interconnection Security Agreements (ISA) should be used for technical requirements, as necessary.[31] These agreements ensure that the partner organizations abide by rules for handling, disclosing, sharing, transmitting, retaining, and using the organization's PII.

PII maintained by the organization should also be reflected in the organization's incident response policies and procedures. A well-defined incident response capability helps the organization detect incidents rapidly, minimize loss and destruction, identify weaknesses, and restore IT operations rapidly. OMB Memorandum M-07-16 sets out specific requirements for reporting incidents involving the loss or inappropriate disclosure of PII. For additional information, see Section 5.

4.1.2 Education, Training, and Awareness

Education, training, and awareness are distinct activities, each critical to the success of privacy and security programs. Their roles related to protecting PII are briefly described below. Additional information on privacy education, training, and awareness is available in NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*.

Awareness efforts are designed to change behavior or reinforce desired PII practices. The purpose of awareness is to focus attention on the protection of PII. Awareness relies on using attention-grabbing techniques to reach all different types of staff across an organization. For PII protection, awareness methods include informing staff of new scams that are being used to steal identities, providing updates on privacy items in the news such as government data breaches and their effect on individuals and the organization, providing examples of how staff members have been held accountable for inappropriate actions, and providing examples of recommended privacy practices.

The goal of training is to build knowledge and skills that will enable staff to protect PII. Laws and regulations may specifically require training for staff, managers, and contractors. An organization should have a training plan and implementation approach, and an organization's leadership should communicate the seriousness of protecting PII to its staff. Organizational policy should define roles and responsibilities for training; training prerequisites for receiving access to PII; and training periodicity and refresher training requirements. To reduce the possibility that PII will be accessed, used, or disclosed inappropriately, all individuals that have been granted access to PII should receive appropriate training and, where applicable, specific role-based training. Depending on the roles and functions involving PII, important topics to address may include:

- The definition of PII
- The basic privacy laws, regulations, and policies that apply to a staff member's organization
- Restrictions on data collection, storage, and use of PII
- Roles and responsibilities for using and protecting PII
- Having the organization's legal counsel or privacy officer determine legal obligations to protect PII

[31] See NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, http://csrc.nist.gov/publications/PubsSPs.html

- Appropriate disposal of PII
- Sanctions for misuse of PII
- Recognizing a security or privacy incident involving PII
- Retention schedules for PII
- Roles and responsibilities in responding to PII-related incidents.

Education develops a common body of knowledge that reflects all of the various specialties and aspects of PII protection. It is used to develop privacy professionals who are able to implement privacy programs that enable their organizations to proactively respond to privacy challenges.

4.2 Privacy-Specific Protection Measures[32]

Privacy-specific protection measures are controls for protecting the confidentiality of PII. These controls provide types of protections not usually needed for other types of data. Privacy-specific protection measures provide additional protections that help organizations collect, maintain, use, and disseminate data in ways that protect the confidentiality of the data.

4.2.1 Minimizing Collection and Retention of PII

The practice of minimizing the collection and retention of PII is a basic privacy principle.[33] By limiting PII collections to the least amount necessary to conduct its mission, the organization may limit potential negative consequences in the event of a data breach involving PII. Organizations should consider the total amount of PII collected and maintained, as well as the types and categories of PII collected and maintained. This general concept is often abbreviated as the "minimum necessary" principle. PII collections should only be made where such collections are essential to meet the authorized business purpose and mission of the organization. If the PII serves no current business purpose, then the PII should no longer be collected.

Also, an organization should regularly review[34] its holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting the organization's business purpose and mission.[35] If the PII is no longer relevant and necessary, then the PII should be properly destroyed. The destruction or disposal of PII must be conducted in accordance with the Federal Records Act and records control schedules approved by the National Archives and Records Administration (NARA).[36] The

[32] Portions of this section were submitted as contributions to the ISO/IEC 29100 *Framework for Privacy* draft standard.

[33] Fair Information Practices are also referred to as privacy principles. See Appendix D for additional information.

[34] The frequency of reviews should be done in accordance with laws, regulations, mandates, and organizational policies that apply to the collection of PII.

[35] The Privacy Act requires that Federal agencies only maintain records relevant and necessary to their mission. Also, OMB directed Federal agencies to review their PII holdings annually and to reduce their holdings to the minimum necessary for proper performance of their missions. OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

[36] The Federal Records Act, 44 U.S.C. § 3301, defines records as "[a]ll books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them." Agencies are required to create and maintain "adequate and proper documentation" of their organization, mission, functions, etc., and may not dispose of records without the approval of the Archivist of the United States. This approval is granted through the General Records Schedules (GRS) and agency specific records schedules.

effective management and prompt disposal of PII, in accordance with NARA-approved disposition schedules, will minimize the risks of unauthorized disclosure.

4.2.2 De-Identifying Information

Full data records are not always necessary, such as for some forms of research, resource planning, and examinations of correlations and trends. The term *de-identified information* is used to describe records that have had enough PII removed or *obscured*, also referred to as masked or obfuscated, such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.[37] De-identified information can be re-identified (rendered distinguishable) by using a code, algorithm, or pseudonym that is assigned to individual records. The code, algorithm, or pseudonym should not be derived from other related information about the individual, and the means of re-identification should only be known by authorized parties and not disclosed to anyone without the authority to re-identify records. A common de-identification technique for obscuring PII is to use a one-way cryptographic function, also known as a hash function, on the PII. De-identified information can be assigned a PII confidentiality impact level of *low*, as long as the following are both true:

- The re-identification algorithm, code, or pseudonym is maintained in a separate system, with appropriate controls in place to prevent unauthorized access to the re-identification information.
- The data elements are not linkable, via public records or other reasonably available external records, in order to re-identify the data.

For example, de-identification could be accomplished by removing account numbers, names, SSNs, and any other identifiable information from a set of financial records. By de-identifying the information, a trend analysis team could perform an unbiased review on those records in the system without compromising the PII or providing the team with the ability to identify any individual. Another example is using health care test results in research analysis. All of the distinguishable PII fields can be removed, and the patient ID numbers can be obscured using pseudo-random data that is linked to a cross-reference table located in a separate system. The only means to reconstruct the original (complete) PII records is through authorized access to the cross-reference table.

Additionally, de-identified information can be aggregated for the purposes of statistical analysis, such as making comparisons, analyzing trends, or identifying patterns. An example is the aggregation and use of multiple sets of de-identified data for evaluating several different types of education loan programs. The data describes characteristics of loan holders, such as age, gender, region, and outstanding loan balances. With this dataset, an analyst could draw statistics showing that 18,000 women in the 30-35 age group have outstanding loan balances greater than $10,000. Although the original data sets contained distinguishable identities for each person and is considered to be PII, the de-identified and aggregated dataset would not contain linked or readily distinguishable data for any individual.

[37] For the purpose of analysis, the definition for de-identified information used in this document is loosely based on the Standard for de-identified data defined in the HIPAA Privacy Rule, and it is generalized to apply to all PII. This definition differs from the HIPAA definition in that it is applied to all PII and does not specifically require the removal of all 18 data elements described by the HIPAA Privacy Rule. The HIPAA Privacy Rule recognizes two ways to de-identify data such that it is no longer considered to be protected health information (PHI). First, 18 specific fields can be removed, such as name, SSN, and phone number. Second, the anonymity of the data can be proven statistically. 45 CFR §164.514, http://www.hhs.gov/ocr/hipaa/finalreg.html

4.2.3 Anonymizing Information

Anonymous is defined as something that cannot be "named or identified." It derives from a Greek word meaning "without a name." [38] Similarly, *anonymized information* is defined as previously identifiable information that has been de-identified and for which a code or other link no longer exists.[39] Anonymized information differs from de-identified information because anonymized information cannot be re-identified. A re-identification algorithm, code, or pseudonym does not exist or has been removed and is not available. Anonymizing information usually involves the application of statistical disclosure limitation techniques[40] to ensure the data cannot be re-identified, such as: [41]

- **Generalizing the Data—**Making information less precise, such as grouping continuous values
- **Suppressing the Data—**Deleting an entire record or certain parts of records
- **Introducing Noise into the Data—**Adding small amounts of variation into selected data
- **Swapping the Data—**Exchanging certain data fields of one record with the same data fields of another similar record (e.g., swapping the zip codes of two records)
- **Replacing Data with the Average Value—**Replacing a selected value of data with the average value for the entire group of data.

Using these techniques, the information is no longer PII, but it can retain its useful and realistic properties.[42]

Anonymized information is useful for system testing.[43] Most systems that are newly developed, newly purchased, or upgraded require testing before being introduced to their intended production environment. Testing generally should simulate real conditions as closely as possible to ensure the new or upgraded system runs correctly and handles the projected system capacity effectively. If PII is used in the test environment, it is required to be protected at the same level that it is protected in the production environment, which can add significantly to the time and expense of testing the system.

Randomly generating fake data in place of PII to test systems is often ineffective because certain properties and statistical distributions of the PII may need to be retained to effectively test the system. There are tools available that substitute PII with synthetic data generated by anonymizing PII. The anonymized information retains the useful properties of the original PII, but the anonymized information is not considered to be PII. Anonymized data substitution is a privacy-specific protection measure that

[38] Merriam Webster Dictionary Online, http://www.merriam-webster.com/dictionary/anonymous.

[39] Based on the Common Rule, which governs confidentiality requirements for research, 45 CFR 46.

[40] Both anonymizing and de-identifying should be conducted by someone with appropriate training. It may be helpful, as appropriate, to consult with a statistician to assess the level of risk with respect to possible unintended re-identification and improper disclosure. For additional information on statistical disclosure limitation techniques, see OMB's Statistical Policy Working Paper #22, http://www.fcsm.gov/working-papers/spwp22.html. See also Census Bureau, *Report on Confidentiality* and Privacy 1790-2002, http://www.census.gov/prod/2003pubs/conmono2.pdf.

[41] The Federal Committee on Statistical Methodology provides a checklist to assist in the assessment of risk for re-identification and improper disclosure. For additional information, see the Federal Committee on Statistical Methodology, Confidentiality and Data Access Committee's Checklist on Disclosure Potential of Data Releases, http://www.fcsm.gov/committees/cdac/.

[42] The retention of useful properties in anonymized data is dependent upon the statistical disclosure limitation technique applied.

[43] Anonymization is also commonly used by agencies to release data sets to the public for research purposes.

enables system testing while reducing the expense and added time of protecting PII. However, not all data can be readily anonymized (e.g. biometric data).

4.3 Security Controls

In addition to the PII-specific protection measures described earlier in this section, many types of technical and operational security controls are available to safeguard the confidentiality of PII. These controls are often already available on a system to protect other types of data processed, stored, or transmitted by the system. The security controls listed in NIST SP 800-53 address general protections of data and systems. The items listed below are some of the NIST SP 800-53 controls that can be used to help safeguard the confidentiality of PII. Note that some of these controls may not be in the recommended set of security controls for the baselines identified in NIST SP 800-53 (e.g., a control might only be recommended for high-impact systems). However, organizations may choose to provide greater protections than what is recommended; see Section 3.1 for a discussion of characteristics to consider when choosing the appropriate controls. In addition to the controls listed below, NIST SP 800-53 contains many other controls that can be used to help protect PII, such as incident response controls.

- **Access Enforcement (AC-3).** Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists). This can be done in many ways. One example is implementing role-based access control and configuring it so that each user can access only the pieces of data necessary for the user's role. Another example is only permitting users to access PII through an application that tightly restricts their access to the PII, instead of permitting users to directly access the databases or files containing PII.[44] Encrypting stored information is also an option for implementing access enforcement.[45] OMB M-07-16 specifies that Federal agencies must "encrypt, using only NIST certified cryptographic modules, all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary or a senior-level individual he/she may designate in writing".
- **Separation of Duties (AC-5).** Organizations can enforce separation of duties for duties involving access to PII. For example, the users of de-identified PII data would not also be in roles that permit them to access the information needed to re-identify the records.
- **Least Privilege (AC-6).** Organizations can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks. Concerning PII, the organization can ensure that users who must access records containing PII only have access to the minimum amount of PII data, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.
- **Remote Access (AC-17).** Organizations can choose to prohibit or strictly limit remote access to PII. If remote access is permitted, the organization can ensure that the communications are encrypted.
- **Access Control for Mobile Devices (AC-19).** Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers

[44] For example, suppose that an organization has a database containing thousands of records on employees' benefits. Instead of allowing a user to have full and direct access to the database, which could allow the user to save extracts of the database records to the user's computer, removable media, or other locations, the organization could permit the user to access only the necessary records and record fields. A user could be restricted to accessing only general demographic information and not any information related to the employees' identities. More information on restricting extracts from PII databases is available in Appendix E.

[45] Additional encryption guidelines and references can be found in FIPS 140-2: *Security Requirements for Cryptographic Modules*, http://csrc.nist.gov/publications/PubsFIPS.html.

at the organization's facilities). Some organizations choose to forbid all telework and remote access involving higher-impact instances of PII so that the information will not leave the organization's physical boundaries. If access is permitted, the organization can ensure that the devices are properly secured and regularly scan the devices to verify their security status (e.g., antivirus software enabled and up-to-date, operating system fully patched).

- **Auditable Events (AU-2).** Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.
- **Audit Monitoring, Analysis, and Reporting (AU-6)**. Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.
- **User Identification and Authentication (IA-2).** Users can be uniquely identified and authenticated before accessing PII.[46] The strength requirement for the authentication mechanism depends on the impact level of the PII and the system as a whole. OMB M-07-16 specifies that Federal agencies must "allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access," and also must "use a 'time-out' function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity."
- **Media Access (MP-2).** Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm). This could also include portable and mobile devices with a storage capability.
- **Media Marking (MP-3).** Organizations can label information system media and output containing PII to indicate how it should be distributed and handled. The organization could exempt specific types of media or output from labeling so long as it remains within a secure environment. Examples of labeling are cover sheets on printouts and paper labels on digital media.
- **Media Storage (MP-4).** Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures. One example is the use of storage encryption technologies to protect PII stored on removable media.
- **Media Transport (MP-5).** Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization's controlled areas. Examples of protective measures are encrypting stored information and locking the media in a container.
- **Media Sanitization (MP-6).** Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.[47] An example is degaussing a hard drive—applying a magnetic field to the drive to render it unusable.
- **Transmission Confidentiality (SC-9).** Organizations can protect the confidentiality of transmitted PII. This is most often accomplished by encrypting the communications or by encrypting the information before it is transmitted.[48]

[46] More information on authentication is available from NIST SP 800-63, *Electronic Authentication Guideline*.

[47] For more information on media sanitization, see NIST SP 800-88, *Guidelines for Media Sanitization*.

[48] NIST has several publications on this topic that are available from http://csrc.nist.gov/publications/PubsSPs.html.

5. Incident Response for Breaches of PII

Handling breaches involving PII is different from regular incident handling and may require additional actions by an organization. Breaches involving PII can receive considerable media attention, which can greatly harm an organization's reputation and reduce the public's trust[49] in the organization. Moreover, affected individuals can be subject to embarrassment, identity theft, or blackmail as the result of a breach of PII. Due to these particular risks of harm, organizations should develop additional policies, such as determining when and how individuals should be notified, when and if a breach should be reported publicly, and whether to provide remedial services, such as credit monitoring, to affected individuals. Organizations should integrate these additional policies into their existing incident handling response policies.

FISMA requires Federal agencies to have procedures for handling information security incidents, and it established a Federal information security incident center to coordinate and share information about incidents, which resulted in the creation of U.S. Computer Emergency Readiness Team (US-CERT). Additionally, NIST provided guidance on security incident handling in NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*. In 2007, OMB issued M-07-16, which provided specific guidance to Federal agencies for handling incidents involving PII.

Incident response plans should be modified to handle breaches involving PII. Incident response plans should also address how to minimize the amount of PII necessary to adequately report and respond to a breach. NIST SP 800-61 Revision 1 describes four phases of handling security incidents. Specific policies and procedures for handling breaches involving PII can be added to each of the following phases identified in NIST SP 800-61: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity. This section provides additional details on PII-specific considerations for each of these four phases.

5.1 Preparation

Preparation requires the most effort because it sets the stage to ensure the PII breach is handled appropriately. Organizations should build their PII breach response plans into their existing incident response plans. The development of PII breach response plans requires organizations to make many decisions about how to handle PII breaches, and the decisions should be used to develop policies and procedures. The policies and procedures should be communicated to the organization's entire staff through training and awareness programs. Training programs should inform employees of the consequences of their actions for inappropriate use and handling of PII.

The organization should determine if existing processes are adequate, and if not establish a new incident reporting method for employees to report suspected or known breaches of PII. The method could be a telephone hotline, email, or a management reporting structure in which employees know to contact a specific person within the management chain. Employees should be able to report any PII breach immediately at any day or time. Additionally, employees should be provided with a clear definition of what constitutes a PII breach and what information needs to be reported. The following information is helpful to obtain from employees who are reporting a known or suspected PII breach:[50]

- Person reporting the incident

[49] According to a 2007 Government Privacy Trust Survey conducted by the Ponemon Institute, a Federal department fell from being a top five most trusted agency in 2006 to just above the bottom five least trusted agencies after the highly publicized breach of millions of PII records in 2006. http://www.govexec.com/dailyfed/0207/022007tdpm1.htm

[50] U.S. Department of Commerce, *Breach Notification Response Plan*, September 28, 2007

- Person who discovered the incident
- Date and time the incident was discovered
- Nature of the incident
- Description of the information lost or compromised
- Storage medium from which information was lost or compromised
- Controls in place to prevent unauthorized use of the lost or compromised information
- Number of individuals potentially affected
- Whether law enforcement was contacted.

Federal agencies are required to report all known or suspected breaches of PII, in any format, to US-CERT within one hour.[51] To meet this obligation, organizations should proactively plan their breach notification response. A PII breach may require notification to persons external to the organization, such as law enforcement, financial institutions, affected individuals, the media, and the public.[52] Organizations should plan in advance how, when, and to whom notifications should be made. Organizations should conduct training sessions on interacting with the media regarding incidents. Additionally, OMB M-07-16 requires federal agencies to include the following elements in their plans for handling breach notification:

- Whether breach notification is required[53]
- Timeliness of the notification
- Source of the notification
- Contents of the notification
- Means of providing the notification
- Who receives the notification; public outreach response.

Additionally, organizations should establish a committee or person responsible for using the breach notification policy to coordinate the organization's response.

The organization should also determine what circumstances require the organization to provide remedial assistance to affected individuals, such as credit monitoring services. The PII confidentiality impact level should be considered for this determination because it provides an analysis of the likelihood of harm for the loss of confidentiality for each instance of PII.

5.2 Detection and Analysis

Organizations may continue to use their current detection and analysis technologies and techniques for handling incidents involving PII. However, adjustments to incident handling processes may be needed, such as ensuring that the analysis process includes an evaluation of whether an incident involves PII.

[51] In M-07-16, OMB required Federal agencies to report all known or suspected PII breaches to US-CERT within one hour.

[52] For additional information about communications with external parties, such as the media, see NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*, http://csrc.nist.gov/publications/PubsSPs.html.

[53] For Federal agencies, notification to US-CERT is always required.

Detection and analysis should focus on both known and suspected breaches of PII. In the event that a suspected breach of PII is detected, Federal agencies should notify US-CERT within one hour.

5.3 Containment, Eradication, and Recovery

Existing technologies and techniques for containment, eradication, and recovery may be used for breaches involving PII. However, changes to incident handling processes may be needed, such as performing additional media sanitization steps when PII needs to be deleted from media during recovery. Particular attention should be paid to using proper forensics techniques[54] to ensure preservation of evidence for intentional criminal acts. Additionally, it is important to determine whether PII was accessed and how many records or individuals were affected.

5.4 Post-Incident Activity

As with other security incidents, information learned through detection, analysis, containment, and recovery should be collected for sharing within the organization and with the US-CERT to help protect against future incidents. The PII breach response plan should be continually updated and improved based on the lessons learned during each incident.

Additionally, the organization should use its PII breach response policy to determine whether the organization should provide affected individuals with remedial assistance, such as credit monitoring. When providing notice to individuals, organizations should make affected individuals aware of their options, such as obtaining a free copy of their credit report, obtaining a freeze credit report, placing a fraud alert on their credit report, or contacting their financial institutions.

[54] For additional information, see NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

Appendix A—Scenarios for PII Identification and Handling

Exercises involving PII scenarios within an organization provide an inexpensive and effective way to build skills necessary to identify potential issues with how the organization identifies and safeguards PII. Individuals who participate in these exercises are presented with a brief PII scenario and a list of general and specific questions related to the scenario. After reading the scenario, the group then discusses each question and determines the most appropriate response for their organization. The goal is to determine what the participants would really do and to compare that with policies, procedures, and generally recommended practices to identify any discrepancies or deficiencies and decide upon appropriate mitigation techniques.

The general questions listed below are applicable to almost any PII scenario. After the general questions are scenarios, each of which is followed by additional scenario-specific questions. Organizations are encouraged to adapt these questions and scenarios for use in their own PII exercises. Also, additional scenarios and questions specific to PII incident handling are available from NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*.[55]

A.1 General Questions

1. What measures are in place to identify, assess, and protect the PII described in the scenario?

2. Which individuals have designated responsibilities within the organization to safeguard the PII described in the scenario?

3. To which people and groups within the organization should questions about PII or the possible misuse of PII be reported?

4. What could happen if the PII described in the scenario is not safeguarded properly?

A.2 Scenarios

Scenario 1: A System Upgrade

An organization is redesigning and upgrading its physical access control systems, which consist of entry-way consoles that recognize ID badges, along with identity management systems and other components. As part of the redesign, several individual physical access control systems are being consolidated into a single system that catalogues and recognizes biometric template data (a facial image and fingerprint), employee name, employee identification number (an internal identification number used by the organization) and employee SSN. The new system will also contain scanned copies of "identity" documentation, including birth certificates, driver's licenses, and/or passports. In addition, the system will maintain a log of all access (authorized or unauthorized) attempts by a badge. The log contains employee identification numbers and timestamps for each access attempt.

1. What information in the system is PII?

2. What is the PII confidentiality impact level? What factors were taken into consideration when making this determination?

[55] SP 800-61 Revision 1 is available at http://csrc.nist.gov/publications/PubsSPs.html.

3. By consolidating data into a single system, does it create additional vulnerabilities that could result in harm to the individual? What additional controls could be put in place to mitigate the risk?

4. Is all of the information necessary for the system to function? Is there a way to minimize the information in the system? Could PII on the system be replaced with operating data that is not PII?

5. Is the organization required to conduct a PIA for this system?

Scenario 2: Protecting Survey Data

Recently, an organization emailed to individuals a link to an online survey, which was designed to gather feedback about the organization's services. The organization identified each individual by name, email address, and an organization-assigned ID number. The majority of survey questions asked individuals to express their satisfaction or dissatisfaction with the organization, but there were also questions asking individuals to provide their zip code along with demographic details on their age, income level, educational background, and marital status.

The following are additional questions for this scenario:

1. Which data elements collected through this survey should be considered PII?

2. What is the PII confidentiality impact level? What factors were taken into consideration when making this determination?

3. How are determinations made as to which data from the survey are relevant to the organization's operations? What happens to data that is deemed unnecessary?

4. What privacy-specific protection measures might help safeguard the PII collected and retained from this survey?

5. What other types of protection measures for safeguarding data (that are not necessarily specific to safeguarding PII) might be used to protect the data from the responses?

Scenario 3: Completing Work at Home

An organization's employee needed to leave early for a doctor's appointment, but the employee was not finished with her work for the day and had no leave time available. Since she had the same spreadsheet application at home, she decided to email a data extract as an attachment to her personal email address and finish her work at home that evening. The data extract was downloaded from an access controlled human resources database located on a server within the organization's security perimeter. The extract contained employee names, identification numbers, dates of birth, salary information, manager's name, addresses, phone numbers, and positions. As she was leaving, she remembered that she had her personal USB flash drive in her purse. She decided the USB drive would be good to use in case she had an attachment problem with the email she had already sent. Although much of the USB drive's space was taken up with family photos she had shared with her coworkers earlier in the day, there was still enough room to add the data extract. She copied the data extract and dropped it in her purse as she left for her appointment. When she arrived home that evening, she plugged the USB drive into her family's computer and used her spreadsheet application to analyze the data.

The following are additional questions for this scenario:

1. Which data elements contained in this data extract should be considered PII?

2. What is the PII confidentiality impact level? What factors were taken into consideration when making this determination?

3. What privacy-specific protection measures might help safeguard the PII contained in the data extract?

4. What should the employee do if her purse (containing the USB drive) is stolen? What should the organization do? How could the employer have prevented this situation?

5. What should the employee do with the copies of the extract when she finishes her work?

6. Should the emailing of the extract to a personal email address be considered a breach? Should storing the data on the personal USB drive be considered a breach?

7. What could the organization do to reduce the likelihood of similar events in the future?

8. How should this scenario be handled if the information is a list of de-identified retirement income statistics? Would the previous questions be answered differently?

Scenario 4: Testing Systems

An organization needed to test an upgrade to its fingerprint matching system before the upgrade could be introduced into the production environment. Because it is difficult to simulate fingerprint image and template data, the organization used real biometric image and template data to test the system. In addition to the fingerprint images and templates, the system also processed the demographic data associated with each fingerprint image, including name, age, sex, race, date of birth, and nationality. After successful completion of the testing, the organization upgraded its production system.

1. Which data elements contained in this system test should be considered PII?

2. What is the PII confidentiality impact level? What factors were taken into consideration when making this determination?

3. What privacy-specific protection measures might help safeguard the PII used in this test?

4. Is a PIA required to conduct this testing? Is a PIA required to complete the production system upgrade?

5. What should the organization do with the data used for testing when it completes the upgrade?

Appendix B—Frequently Asked Questions (FAQ)

Privacy and security leadership and staff, as well as others within organizations, may have questions about identifying, handling, and protecting the confidentiality of personally identifiable information (PII). This appendix contains frequently asked questions (FAQ) related to PII. Organizations are encouraged to customize this FAQ and make it available to their user community.

1. What is personally identifiable information (PII)?

PII is defined in OMB Memorandum M-07-16 as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

2. How does this apply to foreign nationals?

OMB defined the term *individual*, as used in the definition of PII, to mean a citizen of the United States or an alien lawfully admitted for permanent residence, which is based on the Privacy Act definition.[56] For the purpose of protecting the confidentiality of PII, organizations may choose to administratively expand the scope of application to foreign nationals without creating new legal rights. Expanding the scope may reduce administrative burdens and improve operational efficiencies in the protection of data by eliminating the need to maintain separate systems or otherwise separate data. Additionally, the status of citizen, alien, or legal permanent resident can change over time, which makes it difficult to accurately identify and separate the data of foreign nationals. Expanding the scope may also serve additional organizational interests, such as providing reciprocity for data sharing agreements with other organizations.

Agencies may also, consistent with individual practice, choose to extend the protections of the Privacy Act to foreign nationals without creating new judicially enforceable legal rights. For example, DHS has chosen to extend Privacy Act protections (e.g., access, correction), to foreign nationals whose data resides in mixed systems, which are systems of records with information about both U.S. persons and non-U.S. persons.[57]

Organizations should also consult with legal counsel to determine if they have an additional obligation to protect the confidentiality of the personal information relating to foreign nationals, such as the Immigration and Nationality Act, which requires the protection of the confidentiality of Visa applicant data.[58]

3. What does it mean to "distinguish" an individual?

To *distinguish* an individual is to identify an individual. Some examples of information that could distinguish an individual include, but are not limited to, names, passport number, social security number, or biometric image and template.

[56] OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, http://www.whitehouse.gov/omb/memoranda/m03-22.html#1.

[57] *See DHS Privacy Policy Regarding Collection, Use Retention, and Dissemination of Information on Non-U.S. Persons*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.

[58] Immigration and Nationality Act, 8 U.S.C. 1202.

4. What does it mean when a record is "linked"?

A record is *linked* to an individual when it contains information that cannot distinguish an individual when considered separately, but which could distinguish an individual when combined with other data elements present on the same system or a closely-related system. For example, an individual could be identified only by ID #12345 in one database, and another database on the same system could map that ID # to the individual's name and social security number. The records in the first database would be considered "linked" if users were likely to have access to both databases, or could obtain access with minimal effort.

5. What does it mean when a record is "linkable"?

A record is *linkable* to an individual when it contains information that cannot distinguish an individual, but that may be matched or compared with other data elements from a source available to the general public or that is otherwise obtainable. For example, individuals might be identified in a database by home telephone number. The identities of some of the individuals could be determined by comparing this information to publicly available telephone directories.

6. Is personally identifiable information (PII) the same as information in identifiable form (IIF)?

No, the terms PII and IIF are not the same. Their definitions are distinct, cannot be used interchangeably, and have different requirements associated with them.

OMB defines *PII* in OMB Memorandum 07-16 as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

OMB defines *IIF* in OMB Memorandum 03-22 as "information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors)."[59]

The following two distinctions exist between these terms:

- *Indirect identification*. The terms are distinct in how they address the issue of indirect identification. If information does not—by itself—identify an individual, it must be "intended by the agency" to identify an individual in conjunction with other data to meet the definition of IIF. The definition of PII does not address the agency's intent and states that information can be PII even if the data is merely "linkable" to the individual, whether the agency intends to actually link it or not.
- *Scope of policies*. IIF is defined only in terms of identifying the IT systems for which a federal agency must complete a privacy impact assessment (PIA). PII is defined broadly to include personal information stored in any format, both electronic and paper-based.

[59] OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*

7. How did the need for guidelines on protecting PII come about? Why is this important?

The protection of PII is important to maintain public trust and confidence in an organization, to protect the reputation of an organization, and to protect against legal liability for an organization. Organizations have always considered trust, confidence, and reputation as motivating factors in protecting PII. Recently, organizations have become more concerned about the risk of legal liability due to the enactment of many federal, state, and international privacy laws.

In the United States, Federal privacy laws are generally sector-based. For example, the Health Insurance Portability and Accountability Act of 1996 applies to the health care sector, and the Gramm-Leach-Bliley Act of 1999 applies to the financial services sector. In contrast, many states have enacted their own generally applicable privacy laws, such as breach notification laws. Some U.S.-based organizations that conduct business abroad must also comply with international privacy laws, which vary greatly from country to country. Organizations are responsible for determining which laws apply to them based on sector and jurisdiction.

For Federal government agencies, the need to protect PII was first established by the Privacy Act of 1974. It required Federal agencies to protect PII and apply the Fair Information Practices to PII. Also, the Privacy Act required agencies to “establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.”

In response to the increased use of computers and the Internet to process government information, the E-Government Act of 2002 was enacted to ensure public trust in electronic government services. It required Federal agencies to conduct Privacy Impact Assessments (PIAs) and to maintain privacy policies on their web sites. The E-Government Act also directed the OMB to issue implementation guidance to Federal agencies. In 2003, OMB issued M-03-22 to provide guidance on PIAs and web site privacy policies. OMB has continued to provide privacy guidance to Federal agencies on many PII protection topics such as remote access to PII, encryption of PII on mobile devices, and breach notification (see Appendix H for additional information).

Additionally, Federal agencies are required to comply with other privacy laws, such as the Children’s Online Privacy Protection Act (COPPA) and HIPAA (only if the agency acts as a health care provider or other covered entity as defined by the statute).

8. What is the Privacy Act?

The Privacy Act of 1974 is the foundation of public sector privacy law in the U.S. It applies only to Federal agencies and provides a statutory basis for the required use of Fair Information Practices. The Privacy Act pertains only to data maintained within a System of Records (SOR), which means any “group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”[60] Record is defined broadly to include any item of information about an individual, both paper and electronic.

The basic provisions of the Privacy Act include the following:

[60] 5 U.S.C. § 552a (a)(5).

- Provide notice to individuals that explains:[61]
  - The authority for the data collection
  - The purpose of the data collection
  - Routine uses for the data
  - Effects, if any, of not providing the information
- Limit collection of data to the minimum necessary to accomplish the purpose of the agency
- Collect information directly from the person about whom the information pertains, if possible
- Maintain accuracy and completeness of the data
- Disclose the data to only those who need access for proper purposes, such as sharing for an identified routine use or to perform agency work
- Allow individuals to access data pertaining to them, request correction of wrong or incomplete data, and make an appeal for denials of requests for access and correction
- Maintain appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the records.

Violations of the Privacy Act can result in civil and criminal liability.

Information contained within a Privacy Act System of Records usually will be considered PII. Organizations that seek to protect systems (e.g., via security controls) containing PII may be able to realize efficiencies by coordinating with efforts to comply with the Privacy Act, as these activities will often be similar.

9. What is a Privacy Impact Assessment (PIA)? When do I need to conduct a PIA?

The E-Government Act of 2002 required Federal agencies to conduct PIAs, which are processes for identifying and mitigating privacy risks within an information system. If used effectively, a PIA should address risk at every stage of the system development life cycle (SDLC). Most organizations have established their own templates that provide the basis for conducting a PIA. The E-Government Act of 2002 requires Federal agencies to conduct PIAs when:

- Developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
- Initiating a new collection of information that—
  - Will be collected, maintained, or disseminated using information technology; and
  - Includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

[61] The Privacy Act also requires publication of general notice in the Federal Register, which is called a System of Records Notice (SORN).

The E-Government Act authorized OMB to provide Federal agencies with guidance on conducting PIAs, which resulted in OMB Memorandum 03-22. The Memorandum provided examples of system changes that create new privacy risks and trigger the requirement for a new PIA:

- **Conversions**—when paper-based records are to be converted to electronic systems
- **De-Identified to Identifiable**—when functions applied to an existing information collection change de-identified information into information in identifiable form
- **Significant System Management Changes**—when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system
- **Significant Merging**—when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases, or otherwise significantly manipulated
- **New Public Access**—when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public
- **Commercial Sources**—when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources
- **New Interagency Uses—**when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives
- **Internal Flow or Collection**—when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form
- **Alteration in Character of Data**—when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)

The E-Government Act requires publication of PIAs,[62] which must analyze and describe the following information:

- What information is to be collected
- Why the information is being collected
- The intended use of the information
- With whom the information will be shared
- What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent
- How the information will be secured

[62] An agency may exempt itself from this requirement if publication of the PIA would raise national security concerns or reveal classified or sensitive information.

- Whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a
- What choices the agency made regarding an IT system or collection of information as a result of performing the PIA.

10. What is the Paperwork Reduction Act?

The Paperwork Reduction Act (PRA)[63] was passed in 1995, and created a process for the review and approval of Federal government information collections from the public. The purpose of the Act is to minimize the burden of paperwork on the public, minimize the cost of information collections, and increase the quality of Federal information.[64] The PRA requires Federal agencies to get clearance from OMB when an agency plans to collect information from ten or more persons using identical reporting, recordkeeping, or disclosure requirements. The term *persons* is defined broadly to include people, organizations, local government, etc., but it does not include Federal agencies or employees of Federal agencies. Agencies must also provide notice of the collection in the Federal Register before submitting the information collection to OMB for clearance. OMB reviews the proposed information collection and assigns a control number to the collection, which must be displayed on the collection form. A PIA is required for any electronic collection of information that includes PII and requires OMB clearance pursuant to the PRA.

11. What are the general risks to individuals and the organization if PII is misused?

Depending on the type of information lost, an individual may suffer social, economic, or physical harm. If the information lost is sufficient to be exploited by an identity thief, the person can suffer, for example, from a loss of money, damage to credit, a compromise of medical records, threats, and/or harassment. The individual may suffer tremendous losses of time and money to address the damage. Other types of harm that may occur to individuals include denial of government benefits, blackmail, discrimination, and physical harm.

Organizations also face risks to their finances and reputation. If PII is misused, organizations may suffer financial losses in compensating the individuals, assisting them in monitoring their credit ratings, and addressing administrative concerns. In addition, recovering from a major breach is costly to many organizations in terms of time spent by key staff in coordinating and executing appropriate responses. If a loss of PII constitutes a violation of relevant law, the organization and/or its staff may be subject to criminal or civil penalties, or it may have to agree to receive close government scrutiny and oversight. Another major risk to organizations is that their public reputation and public confidence may be lost, potentially jeopardizing the organizations' ability to achieve their missions.

12. What should I consider when reviewing restrictions on collecting PII?

Key considerations to review are any legal requirements that could impact PII collections. One should ask what laws, regulations, and guidance are applicable to the organization considering the type of PII that is collected (e.g., Privacy Act, Paperwork Reduction Act, and the E-Government Act for general PII; HIPAA for health PII; Gramm-Leach-Bliley Act (GLBA) for financial PII; COPPA for children's PII). An organization's legal counsel and privacy officer should always be consulted to determine whether there are restrictions on collecting PII.

[63] PRA, 44 U.S.C. § 3501 et seq.

[64] For additional information, see: http://ocio.os.doc.gov/ITPolicyandPrograms/Information_Collection/dev01_003742.

One could more specifically ask if the collected PII is absolutely necessary to do business (i.e., does it support the business purpose of the system or the organization's mission?) If it does not serve a viable business purpose, then federal agencies may not collect that PII. If the collection of PII does serve a business purpose, then it should be collected, used, shared, and disseminated appropriately.

13. What are examples of PII?

The following examples are meant to offer a cross-section of the types of information that could be considered PII, either singly or collectively, and is not an exhaustive list of all possibilities. Examples of PII records include financial transactions, medical history, criminal history, and employment history. Examples of individual data elements of PII include an individual's name, social security number, passport number, driver's license number, credit card number, vehicle registration or ID number, x-ray, patient ID number, and biometric image and template data (e.g., retina scans, voice signature, facial geometry).[65]

14. What is different about protecting PII compared to any other data and how should PII be protected?

In many cases, protection of PII is similar to protection of other data and includes protecting the confidentiality, integrity, and availability of the information. Most security controls used for other types of data are also applicable to the protection of PII. Also, there are several privacy-specific protection measures, such as anonymization, minimization of PII collection, and de-identification.

In addition to protection requirements for PII, there are other requirements for the handling of PII. The Fair Information Practices provide an overview of these requirements, which include, but are not limited to, notice, consent, access, correction, integrity, and enforcement. Moreover, the factors for assigning a confidentiality impact level to PII are different than other types of data. Breaches to the confidentiality of PII harm both the organization and the individual. Harm to individuals should be factored in strongly because of the magnitude of the potential harm, such as identity theft, embarrassment, and denial of benefits.

[65] Organizations may want to consider how PII relating to deceased individuals should be handled, such as continuing to protect its confidentiality or properly destroying the information. Organizations may want to base their considerations on any obligations to protect, organizational policies, or by evaluation of organization-specific risk factors. With respect to organization-specific risk factors, there is a balancing act because PII relating to deceased individuals can both promote and prevent identity theft. For example, making available lists of deceased individuals can prevent some types of fraud, such as voter fraud. In contrast, PII of a deceased individual also could be used to open a credit card account or to set up a false cover for criminals. Organizations should consult with their legal counsel and privacy officer.

Appendix C—Definitions of Private Information

Various Federal laws, regulations, and guidance documents describe data elements or records about individuals; other terms they define include "information in identifiable form (IIF), "private information," "systems of records," "protected health information (PHI)," and "directory information." Some of these are similar to the definition used in this document for "PII." However, the definition of PII provided in this section should not be confused with any of these other terms, and readers should not assume that the definition used for PII may be used interchangeably with any of these other terms. The table below provides definitions for some of these terms. The table is not intended to be comprehensive, and considers only a few of the Federal authorities with broad effects and applicability.

Information in Identifiable Form (IIF)	E-Government Act of 2002, 44 USC § 208(d).	Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." Information "permitting the physical or online contacting of a specific individual" (see section 208(b)(1)(A)(ii)(II)) is the same as "information in identifiable form."	See Appendix B for further information about the differences between PII and IIF.
Information in Identifiable Form (IIF)	OMB Memorandum 03-22, § II.A.2.	Information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).	OMB 03-22 limits the definition of "individual" to "a citizen of the United States or an alien lawfully admitted for permanent residence," mirroring the Privacy Act definition.
Individually Identifiable Health Information (IIHI)	Health Insurance Portability and Accountability Act of 1996 (HIPAA), The Privacy Rule, 45 CFR § 160.103.	Under the HIPAA Privacy Rule, IIHI is information that is a subset of health information, including demographic information: - Collected from an individual - Created or received by a health care provider, health plan, employer, or health care clearinghouse; - Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and - That identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.	Describes a term applicable only to the HIPAA Privacy and Security Rules; subject to a number of exemptions not made for PII

Term	Defining Authority	Definition	Comments
Protected Health Information (PHI)	Health Insurance Portability and Accountability Act of 1996 (HIPAA), The Security Rule, 45 CFR § 160.103.	Under the HIPAA Security Rule, PHI is individually identifiable health information (IIHI) that is: - Transmitted by electronic media; - Maintained in electronic media; or - Transmitted or maintained in any other form or medium. Protected health information excludes individually identifiable health information in: - Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; - Employment records held by a covered entity in its role as employer.	Describes a term applicable only to the HIPAA Privacy and Security Rules; subject to a number of exemptions not made for PII
Systems of Records	Privacy Act of 1974, 5 U.S.C. § 552a(a)(5).	A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. A record is defined as any item, collection, or grouping of information about an *individual.*	Applies only to Federal agencies. Provides some exemptions for certain types of records. Defines *individual* as limited to citizens of the United States or aliens lawfully admitted for permanent residence.
Education Records	Federal Education Rights Privacy Act, 20 USC § 1232g (a)(4)(A).	Records, files, documents, and other materials which: - contain information directly related to a student; and - are maintained by an educational agency or institution or by a person acting for such agency or institution, subject to some exceptions.	Applies only to educational institutions receiving funds from the Federal government. Exceptions exist for some records maintained for purposes of law enforcement, health, administration, student employment, and others.
Financial Records Non-public personal Information (NPPI)	Gramm-Leach-Bliley Act (GLBA), 15 USC § 6801-6810.	Information collected about consumers: - When consumer is obtaining credit - When entity is performing services in relation to financial product for consumer	Applies only to Financial Institutions, defined as “an entity that regularly provides financial products or financial services to consumers.”

Appendix D—Fair Information Practices

The Fair Information Practices, also known as Privacy Principles, are the framework for most modern privacy laws around the world. Several versions of the Fair Information Practices have been developed through government studies and international organizations. These different versions share common elements, but the elements are divided and expressed differently. The most commonly used versions are discussed in this appendix.[66]

In 1973, the U.S. Department of Health, Education, and Welfare (HEW) (now the Department of Health and Human Services) issued a report entitled *Records, Computers, and the Rights of Citizens* (commonly referred to as the *HEW Report*). The report was the culmination of an extensive study into data processing in the public and private sectors. The HEW Report recommended that Congress enact legislation adopting a "Code of Fair Information Practices" for automated personal data systems. The recommended Fair Information Practices became the foundation for the Privacy Act of 1974. The HEW Report Fair Information Practices included the following:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information is in his or her file and how the information is being used.
- There must be a way for an individual to correct information in his or her records.
- Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse.
- There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.

In 1980, the Organisation for Economic Co-operation and Development (OECD)[67] adopted *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which provide a framework for privacy that has been referenced in U.S. Federal guidance and internationally. The OECD Guidelines, along with the Council of Europe Convention,[68] became the foundation for the European Union's Data Protection Directive.[69] The OECD Guidelines include the following Privacy Principles:

- **Collection Limitation—**There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality—**Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

[66] Portions of this appendix were contributed to and published in the Executive Office of the President, National Science and Technology Council's *Identity Management Task Force Report 2008*, see http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf.

[67] The U.S. is an OECD member country and participated in the development of the OECD Privacy Guidelines, see http://www.ftc.gov/speeches/thompson/thomtacdremarks.shtm.

[68] In 1981, the Council of Europe enacted the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, which also recognized the Fair Information Practices.

[69] In 1995, the European Union enacted the *Data Protection Directive*, Directive 95/46/EC, which required member states to harmonize their national legislation with the terms of the Directive, including the Fair Information Practices. For additional information, see Jody R. Westby, *International Guide to Privacy*, American Bar Association Publishing, 2004.

- **Purpose Specification—**The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

- **Use Limitation—**Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.

- **Security Safeguards—**Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

- **Openness—**There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

- **Individual Participation—**An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

- **Accountability—**A data controller should be accountable for complying with measures which give effect to the principles stated above.

In 2004, the Asia-Pacific Economic Cooperation (APEC) ministers officially endorsed the Privacy Framework[70] developed within one of its committees. The APEC Privacy Framework was based on the OECD Privacy Guidelines, and was developed to encourage electronic commerce among the member states and to build trust with the international community. The Privacy Framework includes the following Privacy Principles:

- **Preventing Harm—**Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.

- **Notice—**Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information.

- **Collection Limitation—**The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.

- **Uses of Personal Information—**Personal information collected should be used only to fulfill the purposes of the collection and other compatible related purposes, except with the consent of the

[70] http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1.

individual, when necessary to provide a product or service requested by the individual, or by authority of law.

- **Choice—**Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.

- **Integrity of Personal Information—**Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.

- **Security Safeguards—**Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.

- **Access and Correction—**Individuals should be able to obtain from the personal information controller confirmation of whether the personal information controller holders personal information about them, have the information provided to them at a reasonable charge and within a reasonable time, and challenge the accuracy of the information, as well as have the information corrected or deleted. Exceptions include situations where the burden would be disproportionate to the risks to the individual's privacy, the information should not be disclosed due to legal or security concerns, and the privacy of other persons would be violated.

- **Accountability—**A personal information controller should be accountable for complying with measures that give effect to the Principles stated above.

Appendix E—Sensitive Database Extracts Technical Frequently Asked Questions

This Frequently Asked Questions (FAQ) document[71] addresses technical aspects associated with implementing the Office of Management and Budget (OMB) requirement to log and verify sensitive database extracts, which was required by OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" which reiterates the log and verify requirement set forward in M-06-16, "Protection of Sensitive Agency Information," issued in June 2006. Topics covered in this FAQ include data extract logging, restrictions, verification, and erasure.

NIST is particularly interested in reviewer suggestions for feasible technical mechanisms for the log and verify requirements. NIST encourages Federal agencies to provide feedback during the public comment period on the possible solutions described in the FAQ and to suggest additional technical solutions.

GENERAL

1. What is the requirement in the OMB memorandum?

The text of the requirement, as stated on page 7 of OMB M-07-16, is "Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required."

2. What is a computer-readable data extract from a database?

This involves retrieving data from a database through a query and saving the data into a separate computer-readable entity such as another database, a spreadsheet, or a text file.

3. What types of information does the requirement apply to?

Although much of M-07-16 focuses on personally identifiable information (PII), the log and verify requirement applies to all sensitive information, including sensitive PII.

4. What is the purpose of the requirement?

The purpose of the requirement is to prevent data extracts containing sensitive information from being accessed by unauthorized parties. This is primarily a concern for mobile devices and removable user media. Ensuring that extracts with sensitive data are erased when they are no longer needed reduces the likelihood of sensitive information being breached.

LOGGING DATA EXTRACTS

5. Which data extracts need to be logged?

All data extracts from databases that are specifically performed by a human, saved to a separate file, and contain sensitive information need to be logged. Machine-to-machine transactions and any transactions that do not result in saving extracts to a file, such as an extract temporarily held in memory, do not need to be logged. If data extracts are well-protected using compensating controls—for example, data extracts

[71] This version of the FAQ is based on the original, which was posted on March 3, 2008 at http://csrc.nist.gov/drivers/documents/OMB/OMB-M-07-16-Data-Extract-FAQ.pdf. The version presented in this appendix includes clarifications from OMB on the intended scope of the requirement, affecting the answers to questions 4, 5, 8, and 12.

are stored on a logically well-secured server in a physically well-secured data center, or stored on properly encrypted media—then log and verify actions may not be necessary.

6. What information should be logged for each extract?

NIST Special Publication (SP) 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems*, specifies an Audit and Accountability (AU) family of technical security controls, which encompasses audit logging requirements. Control number AU-3, Content of Audit Records, states that "audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event." In addition to logging this information for each extract, agencies may also log other types of information. For example, agencies may log whether each data extract contains sensitive information, for future use in determining which extracts need to be erased. Agencies may also describe the purpose and length of time for which extracted sensitive information will be used.

7. What recommendations does NIST provide for logging?

In addition to the audit logging-related security controls specified in NIST SP 800-53 Revision 2, NIST has developed SP 800-92, *Guide to Computer Security Log Management*. SP 800-92 provides recommendations for developing, implementing, and maintaining log management practices throughout an enterprise.

RESTRICTING DATA EXTRACTS

8. How can my agency reduce the number of data extracts that are subject to the requirement?

This can be accomplished by reducing the amount of sensitive information, including sensitive PII, in its databases and by limiting users' ability to perform extracts from databases with sensitive information. Also, as discussed in the answer to question 5, another option is the use of compensating controls.

9. What are some examples of how an agency can reduce the amount of sensitive PII in its databases?

As stated in OMB M-07-16, agencies must collect and retain only the minimum sensitive PII necessary. Agencies may also use de-identification and anonymization techniques to remove sensitive information from database records. These techniques can remove sensitive information permanently, such as replacing PII values with pseudonyms that provide the ability to sort and quantify populations as groups but not individuals. De-identification can also remove PII temporarily, such as mapping PII values to pseudonyms, storing the mappings in a separate file, and replacing the PII values in the database with the pseudonyms. Only an individual with access to both the database and the mapping file could match the individuals' actual identities with the corresponding database records.

10. How can an agency limit users' ability to perform data extracts from databases with sensitive information?

Agencies may grant only authorized users the least access necessary to such databases and to the sensitive information within each database. This could include restricting the types of queries that users can perform and the database fields (for example, social security number) that users can view and include in extracts. Another method is to permit users to access sensitive information in databases only through applications that tightly restrict the users' access to the sensitive information, instead of permitting direct database access. Such applications could manage the data extract process by permitting extracts only when necessary, scrubbing sensitive information, such as sensitive PII, during extraction, forcing all extracts containing sensitive information to be stored centrally, and interacting with centrally-stored extracts on behalf of users so that the users cannot directly access extracts. Agencies may also use other options for limiting data extracts.

11. What technical methods are available for restricting where sensitive extracts are stored?

In addition to the application-based method mentioned above, there are other methods that agencies may use to limit where sensitive extracts are stored. For example, agencies may configure their remote access solutions so as not to permit access to sensitive information databases from mobile devices and non-organization computers (e.g., personally-owned home computers). Agencies could also permit extracts to be stored only on media protected by storage encryption technology. Other methods are more complex and may require considerable planning and deployment time. One example is requiring that sensitive extracts be stored within and accessed only through encrypted virtual machines, which may be set to expire after 90 days. Another example is implementing centralized processing for access to sensitive databases, where the data never leaves the centralized servers and the applications that access the data are run only through thin client solutions.

VERIFYING AND ERASING SENSITIVE DATA EXTRACTS

12. What is required for verifying a sensitive extract?

Agencies may accomplish extract verification through simple checks. An example of such a solution is ad hoc attestation. This involves implementing one or more systems to log the creation of extracts containing sensitive information and to send each extractor a message after 90 days that requires that the extractor either attests to having erased the extract or justifies why the extract is still needed. Agencies may implement more rigorous and formal verification processes than ad hoc attestation to achieve greater confidence in extracts being erased. An example of a more rigorous verification process is storing all extracts on a well-secured centralized system, prohibiting users from directly accessing the extracts, and running a utility that automatically erases extracts 90 days after creation. This assumes that the useful life of the extract ends on the day that it is created; the intent of the requirement is that extracts should be destroyed within 90 days after their useful life ends, which is not necessarily within 90 days of the extract creation date.

13. What is required for erasing a sensitive extract?

The actions needed to erase an extract vary based on the system or media where the extract has been stored. For example, erasing an extract stored on read-only removable media may necessitate physical destruction of the removable media, whereas erasing an extract on a centralized server may involve deleting the extract file and logically sanitizing the portions of the server media that held the file, as well as ensuring that all copies of the extract are properly erased from server backups. Data artifacts from extracts, such as temporary files, may also need to be erased. The procedures for erasing sensitive extracts can result in a significant operational impact on agencies.

14. What other types of technical solutions could be used for sensitive extract verification and erasure?

In addition to the solutions described above, agencies can also implement long-term solutions that automate most of the verification and erasure processes, thus reducing operational impact. Such solutions generally require at least a few years’ effort to implement, so agencies that choose to implement one or more of the long-term solutions may implement one or more of the currently available solutions described above in the meantime. Examples of possible long-term solutions are as follows:

- Use a trusted Digital Rights Management (DRM) platform or similar solution to manage extracts. Such technologies could be used to permit access to each extract for a certain number of days and by particular users, as well as to restrict how each extract can be used (e.g., preventing an extract from being copied or printed). Designing and implementing scalable DRM-type infrastructures and supporting systems for database extract management, including the deployment of client and server applications and platforms that support the chosen technology, is likely to require significant time and resources (at least two years).

- Implement centralized processing for access to sensitive databases using dumb terminals. This is similar to the thin client solution described earlier, except that the dumb terminals have no memory or storage, which prevents any data from being stored locally. Today's versions of “dumb terminals” are actually emulations that run on general-purpose computers, which means that sensitive data could be stored locally. This solution cannot be implemented on a large scale in the near term using current off-the-shelf components.

- Automatically encrypt each extract, centrally manage all the keys, and destroy the keys at the appropriate times to expire the extracts. Identity-based cryptography could extend this scheme to provide finer-grained access control. These methods are currently in the research stage and cannot be implemented in the near term.

Appendix F—Glossary

Selected terms used in the publication are defined below.

Aggregated: Information elements collated on a number of individuals, typically used for the purposes of making comparisons or identifying patterns.

Anonymized Information: Previously identifiable information that has been de-identified and for which a code or other link no longer exists.

Confidentiality: **"**Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information." [44 U.S.C., Sec. 3542, http://uscode.house.gov/download/pls/44C35.txt]

Context of Use: The purpose for which PII is collected, stored, used, processed, disclosed, or disseminated.

De-identified Information: Records that have had enough PII removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information alone can be used to identify an individual.

Distinguishable Information: Information that can be used to identify an individual.

Harm: Any negative or unwanted effects that would be experienced by an individual (i.e., that may be socially, physically, or financially damaging) or an organization if the confidentiality of PII were breached.

Linkable Information: Information that is not sufficient to allow the recipient to distinguish any individual, but that may be matched or compared to information from a secondary data source that is available to the general public or can be otherwise obtained, in order to link together information and potentially distinguish individuals.

Linked Information: Information that is not sufficient to distinguish an individual when considered separately, but which could distinguish an individual when taken collectively or if considered in conjunction with other data elements in the same system or in a closely-related system.

Obscured Data: Data that has been distorted by cryptographic or other means to hide information. It is also referred to as being masked or obfuscated.

Personally Identifiable Information (PII): "Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." [OMB Memorandum 07-16]

PII Confidentiality Impact Level: The level of impact on organizations and individuals should there be a breach of confidentiality involving PII. The possible levels are low, moderate, and high.

Privacy Impact Assessment (PIA): An analysis of how information is handled that ensures handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; determines the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and examines and evaluates protections and alternative processes for handling information to mitigate potential privacy risks.

System of Records: A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Appendix G—Acronyms and Abbreviations

Selected acronyms and abbreviations used in the publication are defined below.

AC	Access Control
APEC	Asia-Pacific Economic Cooperation
CD	Compact Disc
CFR	Code of Federal Regulations
CIPSEA	Confidential Information Protection and Statistical Efficiency Act
COPPA	Children’s Online Privacy Protection Act
DRM	Digital Rights Management
FAQ	Frequently Asked Questions
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	Government Accounting Office
GLBA	Gramm-Leach-Bliley Act
HEW	U.S. Department of Health, Education, and Welfare
HIPAA	Health Insurance Portability and Accountability Act
IA	Identification and Authentication
ID	Identification
IIF	Information in Identifiable Form
IIHI	Individually Identifiable Health Information
IP	Internet Protocol
IPA	Initial Privacy Assessment
IRS	Internal Revenue Service
ISA	Interconnection Security Agreement
IT	Information Technology
ITL	Information Technology Laboratory
MAC	Media Access Control
MP	Media Protection
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NPPI	Non-Public Personal Information
OECD	Organisation for Economic Co-operation and Development
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PDA	Personal Digital Assistant
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PRA	Paperwork Reduction Act

PTA	Privacy Threshold Assessment
SC	System and Communications Protection
SDLC	System Development Life Cycle
SOR	System of Records
SORN	System of Records Notice
SP	Special Publication
SSN	Social Security Number
URL	Uniform Resource Locator
USB	Universal Serial Bus
U.S.C.	United States Code
US-CERT	United States Computer Emergency Response Team

Appendix H—Resources

Those personnel involved with protecting PII and concerned about individual and organizational impact may want to review the following privacy laws and requirements that apply to Federal agencies.[72] Additionally, OMB has issued several memoranda that provide policy guidance and instructions for the implementation of privacy requirements.

Children's Online Privacy Protection Act (COPPA)	http://www.ftc.gov/ogc/coppa1.htm
Confidential Information Protection and Statistical Efficiency Act (CIPSEA)[73]	http://www.whitehouse.gov/omb/inforeg/cipsea/cipsea_statute.pdf
Confidential Information Protection and Statistical Efficiency Act (CIPSEA) Implementation Guidance	http://www.whitehouse.gov/omb/fedreg/2007/061507_cipsea_guidance.pdf
Consolidated Appropriations Act of 2005, Section 522	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h4818enr.txt.pdf
E-Government Act of 2002, Section 208	http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.2458.ENR:
Federal Information Security Management Act (FISMA)[74]	http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.)	http://caselaw.lp.findlaw.com/casecode/uscodes/50/chapters/15/subchapters/iv/sections/section_421.html
FIPS 140-2, *Security Requirements for Cryptographic Modules*	http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*	http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
Freedom of Information Act (FOIA)[75]	http://www.justice.gov/oip/amended-foia-redlined.pdf
Gramm-Leach-Bliley Act (GLBA)	http://thomas.loc.gov/cgi-bin/query/z?c106:S.900.ENR:
Health Insurance Portability and Accountability Act (HIPAA)	http://aspe.hhs.gov/admnsimp/pl104191.htm
Implementing Recommendations of the 9/11 Commission Act of 2007	http://www.govtrack.us/congress/bill.xpd?bill=h110-1
NIST SP 800-30, *Risk Management Guide for Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
NIST SP 800-37 Revision 1 (draft), *Guide for the Security Certification and Accreditation of Federal Information Systems*	http://csrc.nist.gov/publications/drafts/800-37-Rev1/SP800-37-rev1-IPD.pdf
NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

[72] This list is provided for reference only and is not an exhaustive list. For additional information, an organization's legal counsel and privacy officer should be consulted.

[73] CIPSEA is Title V of the E-Government Act of 2002.

[74] FISMA is Title III of the E-Government Act of 2002.

[75] FOIA was recently amended by the *OPEN Government Act of 2007*, Pub. L. No. 110-175 (2007).

Document	URL
NIST SP 800-53 Revision 2, *Recommended Security Controls for Federal Organizations and Information Systems*	http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf
NIST SP 800-60 Revision 1, *Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories*	http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf
NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*	http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
NIST SP 800-63 Version 1.0.2, *Electronic Authentication Guidelines*[76]	http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
Office of Personnel Management (OPM), *Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft*, June 2007	http://www.chcoc.gov/Transmittals/TransmittalDetails.aspx?TransmittalID=847
OMB Circular A-130, *Management of Federal Information Resources*	http://www.whitehouse.gov/omb/circulars/a130/a130.html
OMB Memorandum M-01-05, *Guidance on Inter-agency Sharing of Personal Data – Protecting Personal Privacy*	http://www.whitehouse.gov/omb/memoranda/m01-05.html
OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*	http://www.whitehouse.gov/omb/memoranda/m03-22.html
OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*	http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*	http://www.whitehouse.gov/omb/memoranda/fy2005/m05-08.pdf
OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*	http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-15.pdf
OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*	http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf
OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*	http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-19.pdf
OMB Memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*	http://www.whitehouse.gov/omb/memoranda/fy2006/m06-20.pdf
OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*	http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

[76] NIST 800-63-1 was released as a draft in December 2008, http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf.

Document	URL
OMB Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*	http://www.whitehouse.gov/omb/memoranda/fy2007/m07-19.pdf
OMB Memorandum M-08-09, *New FISMA Privacy Reporting Requirements for FY 2008*	http://www.whitehouse.gov/omb/memoranda/fy2008/m08-09.pdf
OMB Memorandum, September 20, 2006, *Recommendations for Identity Theft Related Data Breach Notification*	http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf
OMB Memorandum, July 2007, *Common Risks Impeding the Adequate Protection of Government Information* (developed jointly with DHS)	http://csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf
Paperwork Reduction Act	http://www.archives.gov/federal-register/laws/paperwork-reduction/
President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 2007	http://www.idtheft.gov/reports/StrategicPlan.pdf
Privacy Act of 1974	http://www.usdoj.gov/oip/privstat.htm
Sensitive Database Extracts Technical Frequently Asked Questions	http://csrc.nist.gov/drivers/documents/OMB/OMB-M-07-16-Data-Extract-FAQ.pdf

President’s Task Force on Identity Theft

The President’s Task Force on Identity Theft was established by Executive Order 13402 on May 10, 2006, launching a new era in the fight against identity theft. Recognizing the heavy financial and emotional toll that identity theft exacts from its victims, and the severe burden it places on the economy, President Bush called for a coordinated approach among government agencies to combat this crime.

The President’s charge was to craft a strategic plan aiming to make the federal government’s efforts more effective and efficient in the areas of identity theft awareness, prevention, detection, and prosecution. To meet that charge, the Task Force, chaired by the Attorney General and co-chaired by the Chairman of the Federal Trade Commission, focused on several areas:

Law Enforcement. The Task Force examined the tools law enforcement can use to prevent, investigate, and prosecute identity theft crimes; recover the proceeds of these crimes; and ensure just and effective punishment of identity thieves.

Education. The Task Force surveyed current education efforts by government agencies and the private sector on how individuals and corporate citizens can protect personal data.

Government safeguards. Because government must help reduce, rather than exacerbate, incidents of identity theft, the Task Force worked with many federal agencies to determine how the government can increase safeguards to better secure the personal data that it and private businesses hold.

The Task Force conducted meetings, spoke with stakeholders, and invited public comment on key issues. The recommendations that comprise the strategic plan are designed to strengthen the efforts of federal, state, and local law enforcement officers; to educate consumers and businesses on deterring, detecting, and defending against identity theft; to assist law enforcement officers in apprehending and prosecuting identity thieves; and to increase the safeguards used by federal agencies and the private sector with respect to the personal data they hold.

Task Force History
The President's Identity Theft Task Force Report, released October 21, 2008.
Combating Identity Theft: A Strategic Plan, released April 23, 2007.
Strategic Plan [PDF]
Volume II: Supplemental Information [PDF]

Identity Theft Task Force Seeks Public Comment
    Comments Submitted to Identity Theft Task Force

President’s Identity Theft Task Force Summary of Interim Recommendations
Press Release: Identity Theft Task Force Announces Interim Recommendation
Fact Sheet: The Work of The President’s Identity Theft Task Force
Executive Order: Strengthening Federal Efforts to Protect Against Identity Theft

Table of Contents

APPENDICES

ENDNOTES

Glossary of Acronyms

AAMVA–American Association of Motor Vehicle Administrators

AARP–American Association of Retired Persons

ABA–American Bar Association

APWG–Anti-Phishing Working Group

BBB–Better Business Bureau

BIN–Bank Identification Number

BJA–Bureau of Justice Assistance

BJS–Bureau of Justice Statistics

CCIPS–Computer Crime and Intellectual Property Section (DOJ)

CCMSI–Credit Card Mail Security Initiative

CFAA–Computer Fraud and Abuse Act

CFTC–Commodity Futures Trading Commission

CIO–Chief Information Officer

CIP–Customer Identification Program

CIRFU–Cyber Initiative and Resource Fusion Center

CMRA–Commercial Mail Receiving Agency

CMS–Centers for Medicare and Medicaid Services (HHS)

CRA–Consumer reporting agency

CVV2–Card Verification Value 2

DBFTF–Document and Benefit Fraud Task Force

DHS–Department of Homeland Security

DOJ–Department of Justice

DPPA–Drivers Privacy Protection Act of 1994

FACT Act–Fair and Accurate Credit Transactions Act of 2003

FBI–Federal Bureau of Investigation

FCD–Financial Crimes Database

FCRA–Fair Credit Reporting Act

FCU Act–Federal Credit Union Act

FDI Act–Federal Deposit Insurance Act

FDIC–Federal Deposit Insurance Corporation

FEMA–Federal Emergency Management Agency

FERPA–Family and Educational Rights and Privacy Act of 1974

FFIEC–Federal Financial Institutions Examination Council

FIMSI–Financial Industry Mail Security Initiative

FinCEN–Financial Crimes Enforcement Network (Department of Treasury)

FISMA–Federal Information Security Management Act of 2002

FRB–Federal Reserve Board of Governors

FSI–Financial Services, Inc.

FTC–Federal Trade Commission

FTC Act–Federal Trade Commission Act

GAO–Government Accountability Office

GLB Act–Gramm-Leach-Bliley Act

HHS–Department of Health and Human Services

HIPAA–Health Insurance Portability and Accountability Act of 1996

IACP–International Association of Chiefs of Police

IAFCI–International Association of Financial Crimes Investigators

IC3–Internet Crime Complaint Center

ICE–U.S. Immigration and Customs Enforcement

IRS–Internal Revenue Service

IRS CI–IRS Criminal Investigation Division

IRTPA–Intelligence Reform and Terrorism Prevention Act of 2004

ISI–Intelligence Sharing Initiative (U.S. Postal Inspection Service)

ISP–Internet service provider

ISS LOB–Information Systems Security Line of Business

ITAC–Identity Theft Assistance Center

ITCI–Information Technology Compliance Institute

ITRC–Identity Theft Resource Center

MCC–Major Cities Chiefs

NAC–National Advocacy Center

NASD–National Association of Securities Dealers, Inc.

NCFTA–National Cyber Forensic Training Alliance

NCHELP–National Council of Higher Education Loan Programs

NCUA–National Credit Union Administration

NCVS–National Crime Victimization Survey

NDAA–National District Attorneys Association

NIH–National Institutes of Health

NIST–National Institute of Standards and Technology

NYSE–New York Stock Exchange

OCC–Office of the Comptroller of the Currency

OIG–Office of the Inspector General

OJP–Office of Justice Programs (DOJ)

OMB–Office of Management and Budget

OPM–Office of Personnel Management

OTS–Office of Thrift Supervision

OVC–Office for Victims of Crime (DOJ)

PCI–Payment Card Industry

PIN–Personal Identification Number

PMA–President's Management Agenda

PRC–Privacy Rights Clearinghouse

QRP–Questionable Refund Program (IRS CI)

RELEAF–Operation Retailers & Law Enforcement Against Fraud

RISS–Regional Information Sharing Systems

RITNET–Regional Identity Theft Network

RPP–Return Preparer Program (IRS CI)

SAR–Suspicious Activity Report

SBA–Small Business Administration

SEC–Securities and Exchange Commission

SMP–Senior Medicare Patrol

SSA–Social Security Administration

SSL–Security Socket Layer

SSN–Social Security number

TIGTA–Treasury Inspector General for Tax Administration

UNCC–United Nations Crime Commission

USA PATRIOT Act–Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Pub. L. No. 107-56)

USB–Universal Serial Bus

US-CERT–United States Computer Emergency Readiness Team

USPIS–United States Postal Inspection Service

USSS–United States Secret Service

VHA–Veterans Health Administration

VOIP–Voice Over Internet Protocol

VPN–Virtual private network

WEDI–Workgroup for Electronic Data Interchange

Identity Theft Task Force Members

Alberto R. Gonzales, Chairman
Attorney General

Deborah Platt Majoras, Co-Chairman
Chairman, Federal Trade Commission

Henry M. Paulson
Department of Treasury

Carlos M. Gutierrez
Department of Commerce

Michael O. Leavitt
Department of Health and Human Services

R. James Nicholson
Department of Veterans Affairs

Michael Chertoff
Department of Homeland Security

Rob Portman
Office of Management and Budget

John E. Potter
United States Postal Service

Ben S. Bernanke
Federal Reserve System

Linda M. Springer
Office of Personnel Management

Sheila C. Bair
Federal Deposit Insurance Corporation

Christopher Cox
Securities and Exchange Commission

JoAnn Johnson
National Credit Union Administration

Michael J. Astrue
Social Security Administration

John C. Dugan
Office of the Comptroller of the Currency

John M. Reich
Office of Thrift Supervision

Alberto R. Gonzales, Chairman
Attorney General

Deborah Platt Majoras, Co-Chairman
Chairman, Federal Trade Commission

Letter to the President

APRIL 11, 2007

The Honorable George W. Bush
President of the United States
The White House
Washington, D.C.

Dear Mr. President:

By establishing the President's Task Force on Identity Theft by Executive Order 13402 on May 10, 2006, you launched a new era in the fight against identity theft. As you recognized, identity theft exacts a heavy financial and emotional toll from its victims, and it severely burdens our economy. You called for a coordinated approach among government agencies to vigorously combat this crime. Your charge to us was to craft a strategic plan aiming to make the federal government's efforts more effective and efficient in the areas of identity theft awareness, prevention, detection, and prosecution. To meet that charge, we examined the tools law enforcement can use to prevent, investigate, and prosecute identity theft crimes; to recover the proceeds of these crimes; and to ensure just and effective punishment of identity thieves. We also surveyed current education efforts by government agencies and the private sector on how individuals and corporate citizens can protect personal data. And because government must help reduce, rather than exacerbate, incidents of identity theft, we worked with many federal agencies to determine how the government can increase safeguards to better secure the personal data that it and private businesses hold. Like you, we spoke to many citizens whose lives have been uprooted by identity theft, and heard their suggestions on ways to help consumers guard against this crime and lessen the burdens of their recovery. We conducted meetings, spoke with stakeholders, and invited public comment on key issues.

The views you expressed in the Executive Order are widely shared. There is a consensus that identity theft's damage is widespread, that it targets all demographic groups, that it harms both consumers and businesses, and that its effects can range far beyond financial harm. We were pleased to learn that many federal departments and agencies, private businesses, and universities are trying to create a culture of security, although some have been faster than others to construct systems to protect personal information.

There is no quick solution to this problem. But, we believe that a coordinated strategic plan can go a long way toward stemming the injuries caused by identity theft and, we hope, putting identity thieves out of business. Taken as a whole, the recommendations that comprise this strategic plan are designed to strengthen the efforts of federal, state, and local law enforcement officers; to educate consumers and businesses on deterring, detecting, and defending against identity theft; to assist law enforcement officers in apprehending and prosecuting identity thieves; and to increase the safeguards employed by federal agencies and the private sector with respect to the personal data with which they are entrusted.

Thank you for the privilege of serving on this Task Force. Our work is ongoing, but we now have the honor, under the provisions of your Executive Order, of transmitting the report and recommendations of the President's Task Force on Identity Theft.

Very truly yours,

Alberto R. Gonzales, Chairman
Attorney General

Deborah Platt Majoras, Co-Chairman
Chairman, Federal Trade Commission

I. Executive Summary

From Main Street to Wall Street, from the back porch to the front office, from the kitchen table to the conference room, Americans are talking about identity theft. The reason: millions of Americans each year suffer the financial and emotional trauma it causes. This crime takes many forms, but it invariably leaves victims with the task of repairing the damage to their lives. It is a problem with no single cause and no single solution.

A. INTRODUCTION

Eight years ago, Congress enacted the Identity Theft and Assumption Deterrence Act,[1] which created the federal crime of identity theft and charged the Federal Trade Commission (FTC) with taking complaints from identity theft victims, sharing these complaints with federal, state, and local law enforcement, and providing the victims with information to help them restore their good name. Since then, federal, state, and local agencies have taken strong action to combat identity theft. The FTC has developed the Identity Theft Data Clearinghouse into a vital resource for consumers and law enforcement agencies; the Department of Justice (DOJ) has prosecuted vigorously a wide range of identity theft schemes under the identity theft statutes and other laws; the federal financial regulatory agencies[2] have adopted and enforced robust data security standards for entities under their jurisdiction; Congress passed, and the Department of Homeland Security issued draft regulations on, the REAL ID Act of 2005; and numerous other federal agencies, such as the Social Security Administration (SSA), have educated consumers on avoiding and recovering from identity theft. Many private sector entities, too, have taken proactive and significant steps to protect data from identity thieves, educate consumers about how to prevent identity theft, assist law enforcement in apprehending identity thieves, and assist identity theft victims who suffer losses.

Over those same eight years, however, the problem of identity theft has become more complex and challenging for the general public, the government, and the private sector. Consumers, overwhelmed with weekly media reports of data breaches, feel vulnerable and uncertain of how to protect their identities. At the same time, both the private and public sectors have had to grapple with difficult, and costly, decisions about investments in safeguards and what more to do to protect the public. And, at every level of government—from the largest cities with major police departments to the smallest towns with one fraud detective—identity theft has placed increasingly pressing demands on law enforcement.

Public comments helped the Task Force define the issues and challenges posed by identity theft and develop its strategic responses. To ensure that the Task Force heard from all stakeholders, it solicited comments from the public.

In addition to consumer advocacy groups, law enforcement, business, and industry, the Task Force also received comments from identity theft victims themselves.[3] The victims wrote of the burdens and frustrations associated with their recovery from this crime. Their stories reaffirmed the need for the government to act quickly to address this problem.

The overwhelming majority of the comments received by the Task Force strongly affirmed the need for a fully coordinated approach to fighting the problem through prevention, awareness, enforcement, training, and victim assistance. Consumers wrote to the Task Force exhorting the public and private sectors to do a better job of protecting their Social Security numbers (SSNs), and many of those who submitted comments discussed the challenges raised by the overuse of Social Security numbers as identifiers. Others, representing certain business sectors, pointed to the beneficial uses of SSNs in fraud detection. The Task Force was mindful of both considerations, and its recommendations seek to strike the appropriate balance in addressing SSN use. Local law enforcement officers, regardless of where they work, wrote of the challenges of multi-jurisdictional investigations, and called for greater coordination and resources to support the investigation and prosecution of identity thieves. Various business groups described the steps they have taken to minimize the occurrence and impact of the crime, and many expressed support for risk-based, national data security and breach notification requirements.

These communications from the public went a long way toward informing the Task Force's recommendation for a fully coordinated strategy. Only an approach that encompasses effective prevention, public awareness and education, victim assistance, and law enforcement measures, and fully engages federal, state, and local authorities will be successful in protecting citizens and private entities from the crime.

B. THE STRATEGY

Although identity theft is defined in many different ways, it is, fundamentally, the misuse of another individual's personal information to commit fraud. Identity theft has at least three stages in its "life cycle," and it must be attacked at each of those stages:

First, the identity thief attempts to acquire a victim's personal information.

Criminals must first gather personal information, either through low-tech methods—such as stealing mail or workplace records, or "dumpster diving" —or through complex and high-tech frauds, such as hacking and the use of malicious computer codes. The loss or theft of personal information by itself, however, does not immediately lead to identity theft. In some cases, thieves who steal personal items inadvertently steal personal information that is stored in or with the stolen personal items, yet never make use of the personal information. It has recently been reported that, during the past year, the personal records of nearly 73 million people have been lost or stolen, but that there is no evidence of a surge in identity theft or financial fraud as a result. Still, because any loss or theft of personal information is troubling and potentially devastating for the persons involved, a strategy to keep consumer data out of the hands of criminals is essential.

Second, the thief attempts to misuse the information he has acquired.

In this stage, criminals have acquired the victim's personal information and now attempt to sell the information or use it themselves. The misuse of stolen personal information can be classified in the following broad categories:

- **Existing account fraud:** This occurs when thieves obtain account information involving credit, brokerage, banking, or utility accounts that are already open. Existing account fraud is typically a less costly, but more prevalent, form of identity theft. For example, a stolen credit card may lead to thousands of dollars in fraudulent charges, but the card generally would not provide the thief with enough information to establish a false identity. Moreover, most credit card companies, as a matter of policy, do not hold consumers liable for fraudulent charges, and federal law caps liability of victims of credit card theft at $50.
- **New account fraud:** Thieves use personal information, such as Social Security numbers, birth dates, and home addresses, to open new accounts in the victim's name, make charges indiscriminately, and then disappear. While this type of identity theft is less likely to occur, it imposes much greater costs and hardships on victims.

In addition, identity thieves sometimes use stolen personal information to obtain government, medical, or other benefits to which the criminal is not entitled.

Third, an identity thief has completed his crime and is enjoying the benefits, while the victim is realizing the harm.

At this point in the life cycle of the theft, victims are first learning of the crime, often after being denied credit or employment, or being contacted by a debt collector seeking payment for a debt the victim did not incur.

In light of the complexity of the problem at each of the stages of this life cycle, the Identity Theft Task Force is recommending a plan that marshals government resources to crack down on the criminals who traffic in stolen identities, strengthens efforts to protect the personal information of our nation's citizens, helps law enforcement officials investigate and prosecute identity thieves, helps educate consumers and businesses about protecting themselves, and increases the safeguards on personal data entrusted to federal agencies and private entities.

The Plan focuses on improvements in four key areas:

- keeping sensitive consumer data out of the hands of identity thieves through better data security and more accessible education;
- making it more difficult for identity thieves who obtain consumer data to use it to steal identities;
- assisting the victims of identity theft in recovering from the crime; and
- deterring identity theft by more aggressive prosecution and punishment of those who commit the crime.

In these four areas, the Task Force makes a number of recommendations summarized in greater detail below. Among those recommendations are the following broad policy changes:

- that federal agencies should reduce the unnecessary use of Social Security numbers (SSNs), the most valuable commodity for an identity thief;
- that national standards should be established to require private sector entities to safeguard the personal data they compile and maintain and to provide notice to consumers when a breach occurs that poses a significant risk of identity theft;
- that federal agencies should implement a broad, sustained awareness campaign to educate consumers, the private sector, and the public sector on deterring, detecting, and defending against identity theft; and
- that a National Identity Theft Law Enforcement Center should be created to allow law enforcement agencies to coordinate their efforts and information more efficiently, and investigate and prosecute identity thieves more effectively.

The Task Force believes that all of the recommendations in this strategic plan—from these broad policy changes to the small steps—are necessary to wage a more effective fight against identity theft and reduce its incidence and damage. Some recommendations can be implemented relatively quickly; others will take time and the sustained cooperation of government entities and the private sector. Following are the recommendations of the President's Task Force on Identity Theft:

PREVENTION: KEEPING CONSUMER DATA OUT OF THE HANDS OF CRIMINALS

Identity theft depends on access to consumer data. Reducing the opportunities for thieves to get the data is critical to fighting the crime. Government, the business community, and consumers have roles to play in protecting data.

Data compromises can expose consumers to the threat of identity theft or related fraud, damage the reputation of the entity that experienced the breach, and carry financial costs for everyone involved. While "perfect security" does not exist, all entities that collect and maintain sensitive consumer information must take reasonable and appropriate steps to protect it.

Data Security in Public Sector

▶ Decrease the Unnecessary Use of Social Security Numbers in the Public Sector by Developing Alternative Strategies for Identity Management

- Survey current use of SSNs by federal government
- Issue guidance on appropriate use of SSNs
- Establish clearinghouse for "best" agency practices that minimize use of SSNs
- Work with state and local governments to review use of SSNs

▶ Educate Federal Agencies on How to Protect Data; Monitor Their Compliance with Existing Guidance

- Develop concrete guidance and best practices
- Monitor agency compliance with data security guidance
- Protect portable storage and communications devices

▶ Ensure Effective, Risk-Based Responses to Data Breaches Suffered by Federal Agencies

- Issue data breach guidance to agencies
- Publish a "routine use" allowing disclosure of information after a breach to those entities that can assist in responding to the breach

Data Security in Private Sector

▶ Establish National Standards for Private Sector Data Protection Requirements and Breach Notice Requirements

▶ Develop Comprehensive Record on Private Sector Use of Social Security Numbers

▶ Better Educate the Private Sector on Safeguarding Data

- Hold regional seminars for businesses on safeguarding information
- Distribute improved guidance for private industry

▶ Initiate Investigations of Data Security Violations

- ▶ **Initiate a Multi-Year Public Awareness Campaign**
  - Develop national awareness campaign
  - Enlist outreach partners
  - Increase outreach to traditionally underserved communities
  - Establish "Protect Your Identity" Days
- ▶ **Develop Online Clearinghouse for Current Educational Resources**

PREVENTION: MAKING IT HARDER TO MISUSE CONSUMER DATA

Because security systems are imperfect and thieves are resourceful, it is essential to reduce the opportunities for criminals to misuse the data they steal. An identity thief who wants to open new accounts in a victim's name must be able to (1) provide identifying information to allow the creditor or other grantor of benefits to access information on which to base a decision about eligibility; and (2) convince the creditor that he is the person he purports to be.

Authentication includes determining a person's identity at the beginning of a relationship (sometimes called verification), and later ensuring that he is the same person who was originally authenticated. But the process can fail: Identity documents can be falsified; the accuracy of the initial information and the accuracy or quality of the verifying sources can be questionable; employee training can be insufficient; and people can fail to follow procedures.

Efforts to facilitate the development of better ways to authenticate consumers without burdening consumers or businesses—for example, multi-factor authentication or layered security—would go a long way toward preventing criminals from profiting from identity theft.

- ▶ **Hold Workshops on Authentication**
  - Engage academics, industry, entrepreneurs, and government experts on developing and promoting better ways to authenticate identity
  - Issue report on workshop findings
- ▶ **Develop a Comprehensive Record on Private Sector Use of SSNs**

VICTIM RECOVERY: HELPING CONSUMERS REPAIR THEIR LIVES

Identity theft can be committed despite a consumer's best efforts at securing information. Consumers have a number of rights and resources available, but some surveys indicate that they are not as well-informed as they could be. Government agencies must work together to ensure that victims have the knowledge, tools, and assistance necessary to minimize the damage and begin the recovery process.

- ▶ **Provide Specialized Training About Victim Recovery to First Responders and Others Offering Direct Assistance to Identity Theft Victims**
  - Train law enforcement officers
  - Provide educational materials for first responders that can be used as a reference guide for identity theft victims
  - Create and distribute an ID Theft Victim Statement of Rights
  - Design nationwide training for victim assistance counselors
- ▶ **Develop Avenues for Individualized Assistance to Identity Theft Victims**
- ▶ **Amend Criminal Restitution Statutes to Ensure That Victims Recover the Value of Time Spent in Trying to Remediate the Harms Suffered**
- ▶ **Assess Whether to Implement a National System That Allows Victims to Obtain an Identification Document for Authentication Purposes**
- ▶ **Assess Efficacy of Tools Available to Victims**
  - Conduct assessment of FACT Act remedies under FCRA
  - Conduct assessment of state credit freeze laws

LAW ENFORCEMENT: PROSECUTING AND PUNISHING IDENTITY THIEVES

Strong criminal law enforcement is necessary to punish and deter identity thieves. The increasing sophistication of identity thieves in recent years has meant that law enforcement agencies at all levels of government have had to increase the resources they devote to investigating related crimes. The investigations are labor-intensive and generally require a staff of detectives, agents, and analysts with multiple skill sets. When a suspected theft involves a large number of potential victims, investigative agencies often need additional personnel to handle victim-witness coordination.

Coordination and Information/Intelligence Sharing

- ▶ **Establish a National Identity Theft Law Enforcement Center**
- ▶ **Develop and Promote the Use of a Universal Identity Theft Report Form**
- ▶ **Enhance Information Sharing Between Law Enforcement and the Private Sector**
  - Enhance ability of law enforcement to receive information from financial institutions
  - Initiate discussions with financial services industry on countermeasures to identity theft
  - Initiate discussions with credit reporting agencies on preventing identity theft

Coordination with Foreign Law Enforcement

- ▶ **Encourage Other Countries to Enact Suitable Domestic Legislation Criminalizing Identity Theft**
- ▶ **Facilitate Investigation and Prosecution of International Identity Theft by Encouraging Other Nations to Accede to the Convention on Cybercrime**
- ▶ **Identify the Nations that Provide Safe Havens for Identity Thieves and Use All Measures Available to Encourage Those Countries to Change Their Policies**
- ▶ **Enhance the United States Government's Ability to Respond to Appropriate Foreign Requests for Evidence in Criminal Cases Involving Identity Theft**
- ▶ **Assist, Train, and Support Foreign Law Enforcement**

Prosecution Approaches and Initiatives

- ▶ **Increase Prosecutions of Identity Theft**
  - Designate an identity theft coordinator for each United States Attorney's Office to design a specific identity theft program for each district
  - Evaluate monetary thresholds for prosecution
  - Encourage state prosecution of identity theft
  - Create working groups and task forces
- ▶ **Conduct Targeted Enforcement Initiatives**
  - Conduct enforcement initiatives focused on using unfair or deceptive means to make SSNs available for sale
  - Conduct enforcement initiatives focused on identity theft related to the health care system
  - Conduct enforcement initiatives focused on identity theft by illegal aliens
- ▶ **Review Civil Monetary Penalty Programs**

Gaps in Statutes Criminalizing Identity Theft

▶ Close the Gaps in Federal Criminal Statutes Used to Prosecute Identity Theft-Related Offenses to Ensure Increased Federal Prosecution of These Crimes

- Amend the identity theft and aggravated identity theft statutes to ensure that identity thieves who misappropriate information belonging to corporations and organizations can be prosecuted
- Add new crimes to the list of predicate offenses for aggravated identity theft offenses
- Amend the statute that criminalizes the theft of electronic data by eliminating the current requirement that the information must have been stolen through interstate communications
- Penalize creators and distributors of malicious spyware and keyloggers
- Amend the cyber-extortion statute to cover additional, alternate types of cyber-extortion

▶ Ensure That an Identity Thief's Sentence Can Be Enhanced When the Criminal Conduct Affects More Than One Victim

Law Enforcement Training

▶ Enhance Training for Law Enforcement Officers and Prosecutors

- Develop course at National Advocacy Center focused on investigation and prosecution of identity theft
- Increase number of regional identity theft seminars
- Increase resources for law enforcement on the Internet
- Review curricula to enhance basic and advanced training on identity theft

Measuring the Success of Law Enforcement

▶ Enhance the Gathering of Statistical Data Impacting the Criminal Justice System's Response to Identity Theft

- Gather and analyze statistically reliable data from identity theft victims
- Expand scope of national crime victimization survey
- Review U.S. Sentencing Commission data
- Track prosecutions of identity theft and resources spent
- Conduct targeted surveys

II. The Contours of the Identity Theft Problem

Every day, too many Americans learn that their identities have been compromised, often in ways and to an extent they could not have imagined. Identity theft victims experience a sense of hopelessness when someone steals their good name and good credit to commit fraud. These victims also speak of their frustration in fighting against an unknown opponent.

Identity theft—the misuse of another individual's personal information to commit fraud—can happen in a variety of ways, but the basic elements are the same. Criminals first gather personal information, either through low-tech methods such as stealing mail or workplace records, or "dumpster diving," or through complex and high-tech frauds such as hacking and the use of malicious computer code. These data thieves then sell the information or use it themselves to open new credit accounts, take over existing accounts, obtain government benefits and services, or even evade law enforcement by using a new identity. Often, individuals learn that they have become victims of identity theft only after being denied credit or employment, or when a debt collector seeks payment for a debt the victim did not incur.

"I was absolutely heartsick to realize our bank accounts were frozen, our names were on a bad check list, and my driver's license was suspended. I hold three licenses in the State of Ohio—my driver's license, my real estate license, and my R.N. license. After learning my driver's license was suspended, I was extremely fearful that my professional licenses might also be suspended as a result of the actions of my imposter."

Maureen Mitchell
Testimony Before
House Committee on
Financial Services,
Subcommittee on
Financial Institutions and
Consumer Credit
June 24, 2003

Individual victim experiences best portray the havoc that identity thieves can wreak. For example, in July 2001, an identity thief gained control of a retired Army Captain's identity when Army officials at Fort Bragg, North Carolina, issued the thief an active duty military identification card in the retired captain's name and with his Social Security number. The military identification, combined with the victim's then-excellent credit history, allowed the identity thief to go on an unhindered spending spree lasting several months. From July to December 2001, the identity thief acquired goods, services, and cash in the victim's name valued at over $260,000. The victim identified more than 60 fraudulent accounts of all types that were opened in his name: credit accounts, personal and auto loans, checking and savings accounts, and utility accounts. The identity thief purchased two trucks valued at over $85,000 and a Harley-Davidson motorcycle for $25,000. The thief also rented a house and purchased a time-share in Hilton Head, South Carolina, in the victim's name.[4]

In another instance, an elderly woman suffering from dementia was victimized by her caregivers, who admitted to stealing as much as $200,000 from her before her death. The thieves not only used the victim's existing credit card accounts, but also opened new credit accounts in her name, obtained financing in her name to purchase new vehicles for themselves, and, using a fraudulent power of attorney, removed $176,000 in U.S. Savings Bonds from the victim's safe-deposit boxes.[5]

In these ways and others, consumers' lives are disrupted and displaced by identity theft. While federal agencies, the private sector, and consumers themselves already have accomplished a great deal to address the causes and impact of identity theft, much work remains to be done. The following strategic plan focuses on a coordinated government response to: strengthen efforts to prevent identity theft; investigate and prosecute identity theft; raise awareness; and ensure that victims receive meaningful assistance.

A. PREVALENCE AND COSTS OF IDENTITY THEFT

There is considerable debate about the prevalence and cost of identity theft in the United States. Numerous studies have attempted to measure the extent of this crime. DOJ, FTC, the Gartner Group, and Javelin Research are just some of the organizations that have published reports of their identity theft surveys.[6] While some of the data from these surveys differ, there is agreement that identity theft exacts a serious toll on the American public.

Although greater empirical research is needed, the data show that annual monetary losses are in the billions of dollars. This includes losses associated with new account fraud, a more costly, but less prevalent form of identity theft, and misuse of existing accounts, a more prevalent but less costly form of identity theft. Businesses suffer most of the direct losses from both forms of identity theft because individual victims generally are not held responsible for fraudulent charges. Individual victims, however, also collectively spend billions of dollars recovering from the effects of the crime.

In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, monetary costs of identity theft include indirect costs to businesses for fraud prevention and mitigation of the harm once it has occurred (e.g., for mailing notices to consumers and upgrading systems). Similarly, individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

Consumers' fears of becoming identity theft victims also may harm our digital economy. In a 2006 online survey conducted by the Business Software Alliance and Harris Interactive, nearly one in three adults (30 percent) said that security fears compelled them to shop online less or not at all during the 2005/2006 holiday season.[7] Similarly, a Cyber Security Industry Alliance survey in June 2005 found that 48 percent of consumers avoided making purchases on the Internet because they feared that their financial information might be stolen.[8] Although no studies have correlated these attitudes with actual online buying habits, these surveys indicate that security concerns likely inhibit some commercial use of the Internet.

In an article entitled "Waitress Gets Own ID When Carding Patron," the Associated Press reported that a bar waitress checking to see whether a patron was old enough to legally drink alcohol was handed her own stolen driver's license, which she reported missing weeks earlier in Lakewood, Ohio. The patron was later charged with identity theft and receiving stolen property.

B. IDENTITY THIEVES: WHO THEY ARE

Unlike some groups of criminals, identity thieves cannot be readily classified. No surveys provide comprehensive data on their primary personal or demographic characteristics. For the most part, victims are not in a good position to know who stole their information or who misused it. According to the FTC's 2003 survey of identity theft, about 14 percent of victims claim to know the perpetrator, who may be a family member, friend, or in-home employee.

Identity thieves can act alone or as part of a criminal enterprise. Each poses unique threats to the public.

Individuals

According to law enforcement agencies, identity thieves often have no prior criminal background and sometimes have pre-existing relationships with the victims. Indeed, identity thieves have been known to prey on people they know, including coworkers, senior citizens for whom they are serving as caretakers, and even family members. Some identity thieves rely on techniques of minimal sophistication, such as stealing mail from homeowners' mailboxes or trash containing financial documents. In some jurisdictions, identity theft by illegal immigrants has resulted in passport, employment, and Social Security fraud. Occasionally, small clusters of individuals with no significant criminal records work together in a loosely knit fashion to obtain personal information and even to create false or fraudulent documents.[9]

A number of recent reports have focused on the connection between individual methamphetamine ("meth") users and identity theft.[10] Law enforcement agencies in Albuquerque, Honolulu, Phoenix, Sacramento, Seattle, and other cities have reported that meth addicts are engaging in identity and data theft through burglaries, mail theft, and theft of wallets and purses. In Salt Lake City, meth users reportedly are organized by white-supremacist gangs to commit identity theft.[11] Tellingly, as meth use has risen sharply in recent years, especially in the western United States, some of the same jurisdictions reporting the highest levels of meth use also suffer from the highest incidence of identity theft. Some state law enforcement officials believe that the two increases might be related, and that identity theft may serve as a major funding mechanism for meth labs and purchases.

In September 2005, a defendant was sentenced by a federal judge in Colorado to a year and one day in prison, and ordered to pay $181,517.05 in restitution, after pleading guilty to the misuse of a Social Security number. The defendant had obtained the identifying information of two individuals, including their SSNs, and used one such identity to obtain a false Missouri driver's license, to cash counterfeit checks, and to open fraudulent credit accounts. The defendant used the second identity to open a fraudulent credit account and to cash fraudulent checks. The case was investigated by the SSA OIG, FBI, U.S. Postal Inspection Service, and the St. Charles, Missouri, Police Department.

Significant Criminal Groups and Organizations

Law enforcement agencies around the country have observed a steady increase in the involvement of groups and organizations of repeat offenders or career criminals in identity theft. Some of these groups—including national gangs such as Hell's Angels and MS-13—are formally organized, have a hierarchical structure, and are well-known to law enforcement because of their longstanding involvement in other major crimes such as drug trafficking. Other groups are more loosely-organized and, in some cases, have taken advantage of the Internet to organize, contact each other, and coordinate their identity theft activities more efficiently. Members of these groups often are located in different countries and communicate primarily via the Internet. Other groups have a real-world connection with one another and share a nationality or ethnic group.

Law enforcement agencies also have seen increased involvement of foreign organized criminal groups in computer- or Internet-related identity theft schemes. In Asia and Eastern Europe, for example, organized groups are increasingly sophisticated both in the techniques they use to deceive Internet users into disclosing personal data, and in the complexity of tools they use, such as keyloggers (programs that record every keystroke as an Internet user logs onto his computer or a banking website), spyware (software that covertly gathers user information through the user's Internet connection, without the user's knowledge), and botnets (networks of computers that criminals have compromised and taken control of for some other purpose, ranging from distribution of spam and malicious computer code to attacks on other computers). According to law enforcement agencies, such groups also are demonstrating increasing levels of sophistication and specialization in their online crime, even selling goods and services—such as software templates for making counterfeit identification cards and payment card magnetic strip encoders—that make the stolen data even more valuable to those who have it.

C. HOW IDENTITY THEFT HAPPENS: THE TOOLS OF THE TRADE

Consumer information is the currency of identity theft, and perhaps the most valuable piece of information for the thief is the SSN. The SSN and a name can be used in many cases to open an account and obtain credit or other benefits in the victim's name. Other data, such as personal identification numbers (PINs), account numbers, and passwords, also are valuable because they enable thieves to access existing consumer accounts.

Identity theft is prevalent in part because criminals are able to obtain personal consumer information everywhere such data are located or stored. Homes and businesses, cars and health-club lockers, electronic networks, and even trash baskets and dumpsters have been targets for identity thieves. Some

In July 2003, a Russian computer hacker was sentenced in federal court to a prison term of four years for supervising a criminal enterprise in Russia dedicated to computer hacking, fraud, and extortion. The defendant hacked into the computer system of Financial Services, Inc. (FSI), an internet web hosting and electronic banking processing company located in Glen Rock, New Jersey, and stole 11 passwords used by FSI employees to access the FSI computer network as well as a text file containing approximately 3,500 credit card numbers and associated card holder information for FSI customers. One of the defendant's accomplices then threatened FSI that the hacker group would publicly release this stolen credit card information and hack into and further damage the FSI computer system unless FSI paid $6,000. After a period of negotiation, FSI eventually agreed to pay $5,000.
In sentencing the defendant, the federal judge described the scheme as an "unprecedented, wide-ranging, organized criminal enterprise" that "engaged in numerous acts of fraud, extortion, and intentional damage to the property of others, involving the sophisticated manipulation of computer data, financial information, and credit card numbers." The court found that the defendant was responsible for an aggregate loss to his victims of approximately $25 million.

thieves use more technologically-advanced means to extract information from computers, including malicious-code programs that secretly log information or give criminals access to it.

The following are among the techniques most frequently used by identity thieves to steal the personal information of their victims.

Common Theft and Dumpster Diving

While often considered a "high tech" crime, data theft often is no more sophisticated than stealing paper documents. Some criminals steal documents containing personal information from mail boxes; indeed, mail theft appears to be a common way that meth users and producers obtain consumer data.[12] Other identity thieves simply take documents thrown into unprotected trash receptacles, a practice known as "dumpster diving."[13] Still others steal information using techniques no more sophisticated than purse snatching.

Progress is being made in reducing the opportunities that identity thieves have to obtain personal information in these ways. The Fair and Accurate Credit Transactions Act of 2003 (FACT Act)[14] requires merchants that accept

A ramp agent for a major airline participated in a scheme to steal financial documents, including checks and credit cards, from the U.S. mail at Thurgood Marshall Baltimore-Washington International Airport and transfer those financial documents to his co-conspirators for processing. The conspirators used the documents to obtain cash advances and withdrawals from lines of credit. In September 2005, a federal judge sentenced the ramp agent to 14 years in prison and ordered him to pay $7 million in restitution.

Partial display of credit cards, checks, and identifying documents seized in federal investigation of identity theft ring in Maryland, 2005.
Source: U.S. Department of Justice

credit or debit cards to truncate the numbers on receipts that are electronically printed—a measure that is intended, among other things, to reduce the ability of a "dumpster diver" to obtain a victim's credit card number simply by looking through that victim's discarded trash. Merchants had a period of time to comply with that requirement, which now is in full effect.[15]

Employee/Insider Theft

Dishonest insiders can steal sensitive consumer data by removing paper documents from a work site or accessing electronic records. Criminals also may bribe insiders, or become employees themselves to access sensitive data at companies. The failure to disable a terminated employee's access to a computer system or confidential databases contained within the system also could lead to the compromise of sensitive consumer data. Many federal agencies have taken enforcement actions to punish and deter such insider compromise.

In December 2003, the Office of the Comptroller of the Currency (OCC) directed a large financial institution to improve its employee screening policies, procedures, systems, and controls after finding that the institution had inadvertently hired a convicted felon who used his new post to engage in identity theft-related crimes. Deficiencies in the institution's screening practices came to light through the OCC's review of the former employee's activities.

Electronic Intrusions or Hacking

Hackers steal information from public and private institutions, including large corporate databases and residential wireless networks. First, they can intercept data during transmission, such as when a retailer sends payment card information to a card processor. Hackers have developed tools to penetrate firewalls, use automated processes to search for account data or other personal information, export the data, and hide their tracks.[16] Several recent government enforcement actions have targeted this type of data theft.

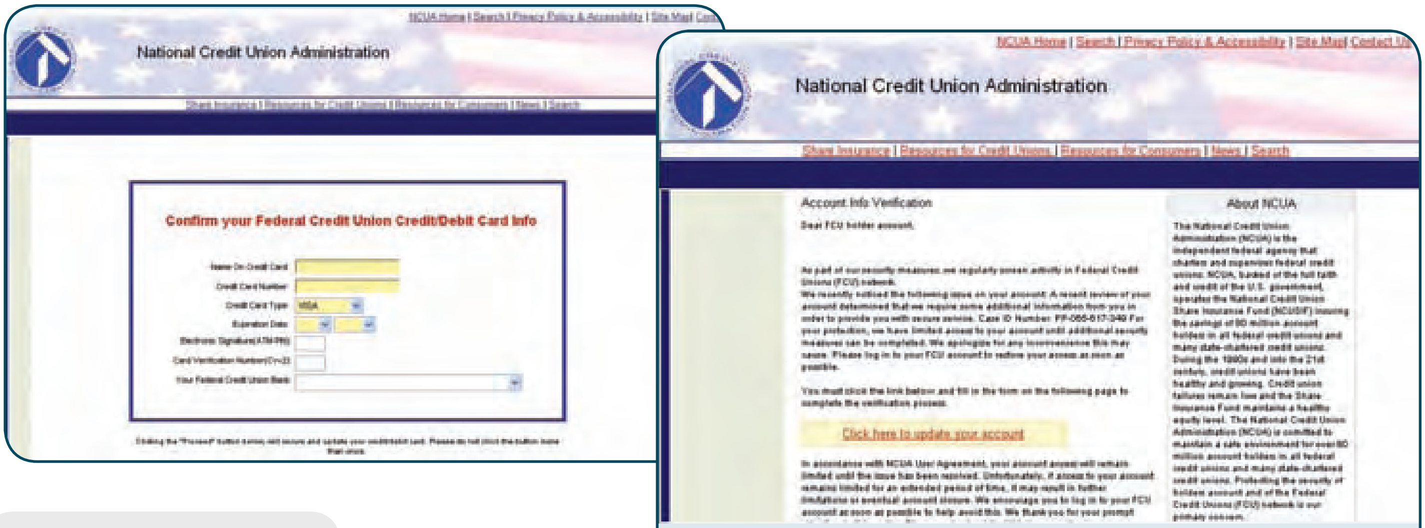
Second, hackers also can gain access to underlying applications—programs used to "communicate" between Internet users and a company's internal databases, such as programs to retrieve product information. One research firm estimates that nearly 75 percent of hacker attacks are targeted at the application, rather than the network.[17] It is often difficult to detect the hacker's application-level activities, because the hacker connects to the website through the same legitimate route any customer would use, and the communication is thus seen as permissible activity.

According to the Secret Service, many major breaches in the credit card system in 2006 originated in the Russian Federation and the Ukraine, and criminals operating in those two countries have been directly involved in some of the largest breaches of U.S. financial systems for the past five years.

In December 2004, a federal district judge in North Carolina sentenced a defendant to 108 months in prison after he pleaded guilty to crimes stemming from his unauthorized access to the nationwide computer system used by the Lowe's Corporation to process credit card transactions. To carry out this scheme, the defendant and at least one other person secretly compromised the wireless network at a Lowe's retail store in Michigan and gained access to Lowe's central computer system. The defendant then installed a computer program designed to capture customer credit card information on the computer system of several Lowe's retail stores. After an FBI investigation of the intrusion, the defendant and a confederate were charged.

Social Engineering: Phishing, Malware/Spyware, and Pretexting

Identity thieves also use trickery to obtain personal information from unwitting sources, including from the victim himself. This type of deception, known as "social engineering," can take a variety of forms.



NCUA Home | Search | Privacy Policy & Accessibility | Site Map | Contact Us

National Credit Union Administration

Share Insurance | Resources for Credit Unions | Resources for Consumers | News | Search

Confirm your Federal Credit Union Credit/Debit Card Info

Name On Credit Card

Credit Card Number

Credit Card Type VISA

Expiration Date

Electronic Signature(ATM PIN)

Card Verification Number(Cvv2)

Your Federal Credit Union Bank

Clicking the "Proceed" button below will secure and update your credit/debit card. Please do not click the button more than once.

Account Info Verification

Dear FCU holder account,

As part of our security measures, we regularly screen activity in Federal Credit Unions (FCU) network.
We recently noticed the following issue on your account: A recent review of your account determined that we require some additional information from you in order to provide you with secure service. Case ID Number: PP-055-617-349 For your protection, we have limited access to your account until additional security measures can be completed. We apologize for any inconvenience this may cause. Please log in to your FCU account to restore your access as soon as possible.

You must click the link below and fill in the form on the following page to complete the verification process.

Click here to update your account

In accordance with NCUA User Agreement, your account access will remain limited until the issue has been resolved. Unfortunately, if access to your account remains limited for an extended period of time, it may result in further limitations or eventual account closure. We encourage you to log in to your FCU account as soon as possible to help avoid this. We thank you for your prompt

About NCUA

The National Credit Union Administration (NCUA) is the independent federal agency that charters and supervises federal credit unions. NCUA, backed of the full faith and credit of the U.S. government, operates the National Credit Union Share Insurance Fund (NCUSIF) insuring the savings of 80 million account holders in all federal credit unions and many state-chartered credit unions. During the 1990s and into the 21st century, credit unions have been healthy and growing. Credit union failures remain low and the Share Insurance Fund maintains a healthy equity level. The National Credit Union Administration (NCUA) is committed to maintain a safe environment for over 80 million account holders in all federal credit unions and many state-chartered credit unions. Protecting the security of holders account and of the Federal Credit Unions (FCU) network is our primary concern.

"Phishing" Email and Associated Website Impersonating National Credit Union Administration Email and Website
Source: Anti-Phishing Working Group

At the beginning of the 2006 tax filing season, identity thieves sent emails that purported to originate from the IRS's website to taxpayers, falsely informing them that there was a problem with their tax refunds. The emails requested that the taxpayers provide their SSNs so that the IRS could match their identities to the proper tax accounts. In fact, when the users entered their personal information – such as their SSNs, website usernames and passwords, bank or credit-card account numbers and expiration dates, among other things – the phishers simply harvested the data at another location on the Internet. Many of these schemes originated abroad, particularly in Eastern Europe. Since November 2005, the Treasury Inspector General for Tax Administration (TIGTA) and the IRS have received over 17,500 complaints about phishing scams, and TIGTA has identified and shut down over 230 phishing host sites targeting the IRS.

Phishing: "Phishing" is one of the most prevalent forms of social engineering. Phishers send emails that appear to be coming from legitimate, well-known sources—often, financial institutions or government agencies. In one example, these email messages tell the recipient that he must verify his personal information for an account or other service to remain active. The emails provide a link, which goes to a website that appears legitimate. After following the link, the web user is instructed to enter personal identifying information, such as his name, address, account number, PIN, and SSN. This information is then harvested by the phishers. In a variant of this practice, victims receive emails warning them that to avoid losing something of value (e.g., Internet service or access to a bank account) or to get something of value, they must click on a link in the body of the email to "reenter" or "validate" their personal data. Such phishing schemes often mimic financial institutions' websites and emails, and a number of them have even mimicked federal government agencies to add credibility to their demands for information. Additionally, phishing recently has taken on a new form, dubbed "vishing," in which the thieves use Voice Over Internet Protocol (VOIP) technology to spoof the telephone call systems of financial institutions and request callers provide their account information.[18]

Malware/Spyware/Keystroke Loggers: Criminals also can use spyware to illegally gain access to Internet users' computers and data without the users' permission. One email-based form of social engineering is the use of enticing emails offering free pornographic images to a group of victims; by opening the email, the victim launches the installation of malware, such as spyware or keystroke loggers, onto his computer. The keystroke loggers gather and send information on the user's Internet sessions back to the hacker, including user names and passwords for financial accounts and other personal information. These sophisticated methods of accessing personal information through malware have supplemented other long-established methods by which criminals obtain victims' passwords and other useful data—such as "sniffing" Internet traffic, for example, by listening to network traffic on a shared physical network, or on unencrypted or weakly encrypted wireless networks.

Pretexting: Pretexting[19] is another form of social engineering used to obtain sensitive information. In many cases, pretexters contact a financial institution or telephone company, impersonating a legitimate customer, and request that customer's account information. In other cases, the pretext is accomplished by an insider at the financial institution, or by fraudulently opening an online account in the customer's name.[20]

Stolen Media

In addition to instances of deliberate theft of personal information, data also can be obtained by identity thieves in an "incidental" manner. Criminals frequently steal data storage devices, such as laptops or portable media, that contain personal information.[21] Although the criminal originally targeted the hardware, he may discover the stored personal information and realize its value and possibility for exploitation. Unless adequately safeguarded—such as through the use of technological tools for protecting data—this information can be accessed and used to steal the victim's identity. Identity thieves also may obtain consumer data when it is lost or misplaced.

Failure to "Know Your Customer"

Data brokers compile consumer information from a variety of public and private sources and then offer it for sale to different entities for a range of purposes. For example, government agencies often purchase consumer information from data brokers to locate witnesses or beneficiaries, or for law enforcement purposes. Identity thieves, however, can steal personal information from data brokers who fail to ensure that their customers have a legitimate need for the data.

The Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLB Act) impose specific duties on certain types of data brokers that disseminate particular types of information.[22] For example, the FCRA requires data brokers that are consumer reporting agencies to make reasonable efforts to verify the identity of their customers and to ensure that those customers have a permissible purpose for obtaining the information. The GLB Act limits the ability of a financial institution to resell covered financial information.

Existing laws, however, do not reach every kind of personal information collected and sold by data brokers. In addition, when data brokers fail to comply with their statutory duties, they open the door to criminals who can access the personal information held by the data brokers by exploiting poor customer verification practices.

In January 2006, the FTC settled a lawsuit against data broker ChoicePoint, Inc., alleging that it violated the FCRA when it failed to perform due diligence in evaluating and approving new customers. The FTC alleged that ChoicePoint approved as customers for its consumer reports identity thieves who lied about their credentials and whose applications should have raised obvious red flags. Under the settlement, ChoicePoint paid $10 million in civil penalties and $5 million in consumer redress and agreed to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to establish a comprehensive information security program, and to obtain audits by an independent security professional every other year until 2026.

A "skimmer"
Source: Durham, Ontario Police

"Skimming"

Because it is possible to use someone's credit account without having physical access to the card, identity theft is easily accomplished when a criminal obtains a receipt with the credit account number, or uses other technology to collect that account information.[23] For example, over the past several years, law enforcement authorities have witnessed a substantial increase in the use of devices known as "skimmers." A skimmer is an inexpensive electronic device with a slot through which a person passes or "skims" a credit or debit card. Similar to the device legitimate businesses use in processing customer card payments, the skimmer reads and records the magnetically encoded data on the magnetic stripe on the back of the card. That data then can be downloaded either to make fraudulent copies of real cards, or to make purchases when the card is not required, such as online. A retail employee, such as a waiter, can easily conceal a skimmer until a customer hands him a credit card. Once he is out of the customer's sight, he can skim the card through the device, and then swipe it through the restaurant's own card reader to generate a receipt for the customer to sign. The waiter then can pass the recorded data to an accomplice, who can encode the data on blank cards with magnetic stripes. A variation of skimming involves an ATM-mounted device that is able to capture the magnetic information on the consumer's card, as well as the consumer's password.

In March 2006, a former candidate for the presidency of Peru pleaded guilty in a federal district court to charges relating to a large-scale credit card fraud and money laundering conspiracy. The defendant collected stolen credit card numbers from people in Florida who had used skimmers to obtain the information from customers of retail businesses where they worked, such as restaurants and rental car companies. He used some of the credit card fraud proceeds to finance various trips to Peru during his candidacy.

D. WHAT IDENTITY THIEVES DO WITH THE INFORMATION THEY STEAL: THE DIFFERENT FORMS OF IDENTITY THEFT

Once they obtain victims' personal information, criminals misuse it in endless ways, from opening new accounts in the victim's name, to accessing the victim's existing accounts, to using the victim's name when arrested. Recent survey data show that misuse of existing credit accounts, however, represents the single largest category of fraud.

Misuse of Existing Accounts

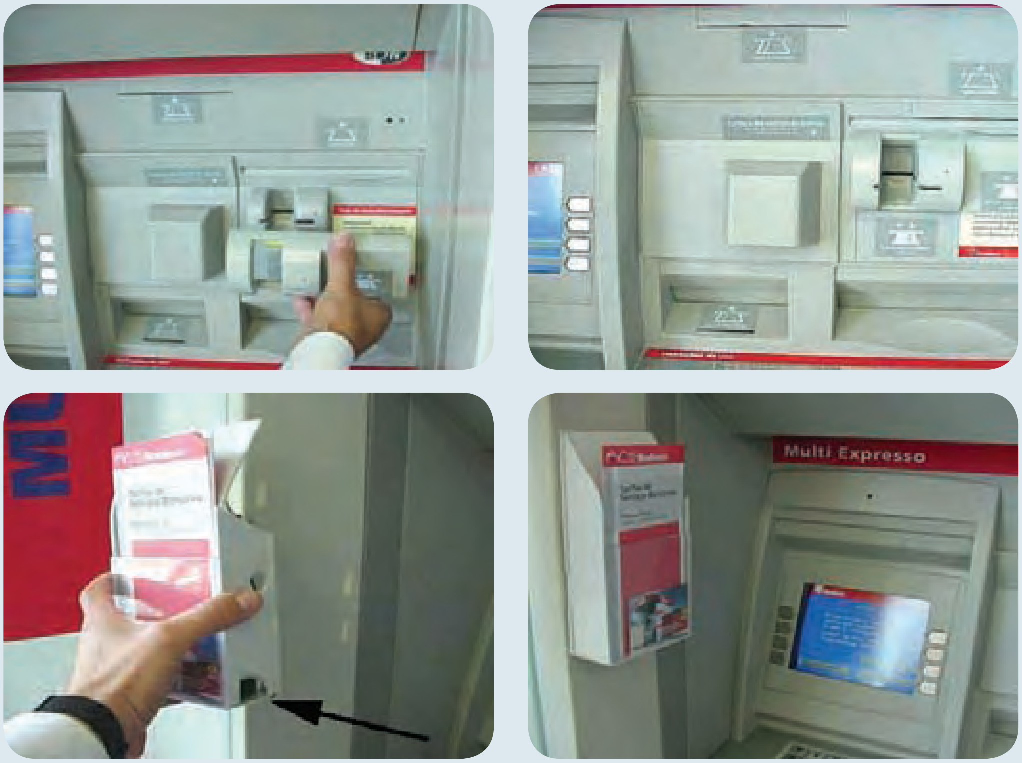
Misuse of existing accounts can involve credit, brokerage, banking, or utility accounts, among others. The most common form, however, involves credit accounts. This occurs when an identity thief obtains either the actual credit card, the numbers associated with the account, or the information derived from the magnetic strip on the back of the card. Because it is possible to make charges through remote purchases, such as online sales or by telephone, identity thieves are often able to commit fraud even as the card remains in the consumer's wallet.

Recent complaint data suggest an increasing number of incidents involving unauthorized access to funds in victims' bank accounts, including checking accounts—sometimes referred to as "account takeovers."[24] The Postal Inspection Service reports that it has seen an increase in account takeovers originating outside the United States. Criminals also have attempted to access funds in victims' online brokerage accounts.[25]

Federal law limits the liability consumers face from existing account misuse, generally shielding victims from direct losses due to fraudulent charges to their accounts. Nevertheless, consumers can spend many hours disputing the charges and making other corrections to their financial records.[26]

New Account Fraud

A more serious, if less prevalent, form of identity theft occurs when thieves are able to open new credit, utility, or other accounts in the victim's name, make charges indiscriminately, and then disappear. Victims often do not learn of the fraud until they are contacted by a debt collector or are turned down for a loan, a job, or other benefit because of a negative credit rating. While this is a less prevalent form of fraud, it causes more financial harm, is less likely to be discovered quickly by its victims, and requires the most time for recovery.



Criminal's skimmer, mounted and colored to resemble exterior of real ATM. A pinhole camera is mounted inside a plastic brochure holder to capture customer's keystrokes.
Source: University of Texas Police Department

In December 2005, a highly organized ring involved in identity theft, counterfeit credit and debit card fraud, and fencing of stolen products was shut down when Postal Inspectors and detectives from the Hudson County, New Jersey, Prosecutor's Office arrested 13 of its members. The investigation, which began in June 2005, uncovered more than 2,000 stolen identities and at least $1.3 million worth of fraudulent transactions. The investigation revealed an additional $1 million in fraudulent credit card purchases in more than 30 states and fraudulent ATM withdrawals. The account information came from computer hackers outside the United States who were able to penetrate corporate databases. Additionally, the ring used counterfeit bank debit cards encoded with legitimate account numbers belonging to unsuspecting victims to make fraudulent withdrawals of hundreds of thousands of dollars from ATMs in New Jersey, New York, and other states.

When criminals establish new credit card accounts in others' names, the sole purpose is to make the maximum use of the available credit from those accounts, whether in a short time or over a longer period. By contrast, when criminals establish new bank or loan accounts in others' names, the fraud often is designed to obtain a single disbursement of funds from a financial institution. In some cases, the criminal deposits a check drawn on an account with insufficient funds, or stolen or counterfeit checks, and then withdraws cash.

Federal identity theft charges were brought against 148 illegal aliens accused of stealing the identities of lawful U.S. citizens in order to gain employment. The aliens being criminally prosecuted were identified as a result of Operation Wagon Train, an investigation led by agents from U.S. Immigration and Customs Enforcement (ICE), working in conjunction with six U.S. Attorney's Offices. Agents executed civil search warrants at six meat processing plants. Numerous alien workers were arrested, and many were charged with aggravated identity theft, state identity theft, or forgery. Many of the names and Social Security numbers being used at the meat processing plants were reported stolen by identity theft victims to the FTC. In many cases, victims indicated that they received letters from the Internal Revenue Service demanding back taxes for income they had not reported because it was earned by someone working under their name. Other victims were denied driver's licenses, credit, or even medical services because someone had improperly used their personal information before.

"Brokering" of Stolen Data

Law enforcement has also witnessed an increase in the marketing of personal identification data from compromised accounts by criminal data brokers. For example, certain websites, known as "carding sites," traffic in large quantities of stolen credit-card data. Numerous individuals, often located in different countries, participate in these carding sites to acquire and review newly acquired card numbers and supervise the receipt and distribution of those numbers. The Secret Service calculated that the two largest current carding sites collectively have nearly 20,000 member accounts.

Immigration Fraud

In various parts of the country, illegal immigrants use fraudulently obtained SSNs or passports to obtain employment and assimilate into society. In extreme cases, an individual SSN may be passed on to and used by many illegal immigrants.[27] Although victims of this type of identity theft may not necessarily suffer financial harm, they still must spend hour upon hour attempting to correct their personal records to ensure that they are not mistaken for an illegal immigrant or cheated out of a government benefit.

Medical Identity Theft

Recent reports have brought attention to the problem of medical identity theft, a crime in which the victim's identifying information is used to obtain or make false claims for medical care.[28] In addition to the financial harm associated with other types of identity theft, victims of medical identity theft may have their health endangered by inaccurate entries in their medical records. This inaccurate information can potentially cause victims to receive improper medical care, have their insurance depleted, become ineligible for health or life insurance, or become disqualified from some jobs. Victims may not even be aware that a theft has occurred because medical identity theft can be difficult to discover, as few consumers regularly review their medical records, and victims may not realize that they have been victimized until they receive collection notices, or they attempt to seek medical care themselves, only to discover that they have reached their coverage limits.

Other Frauds

Identity theft is inherent in numerous other frauds perpetrated by criminals, including mortgage fraud and fraud schemes directed at obtaining government benefits, including disaster relief funds. The IRS's Criminal Investigation Division, for example, has seen an increase in the use of stolen SSNs to file tax returns. In some cases, the thief files a fraudulent return seeking a refund before the taxpayer files. When the real taxpayer files, the IRS may not accept his return because it is considered a duplicate return. Even if the taxpayer ultimately is made whole, the government suffers the loss from paying multiple refunds.

With the advent of the prescription drug benefit of Medicare Part D, the Department of Health and Human Services' Office of the Inspector General (HHS OIG) has noted a growing incidence of health care frauds involving identity theft. These frauds include telemarketers who fraudulently solicit potential Medicare Part D beneficiaries to disclose information such as their Health Insurance Claim Number (which includes the SSN) and bank account information, as well as marketers who obtain identities from nursing homes and other adult care facilities (including deceased beneficiaries and severely cognitively impaired persons) and use them fraudulently to enroll unwilling beneficiaries in alternate Part D plans in order to increase their sales commissions. The types of fraud that can be perpetrated by an identity thief are limited only by the ingenuity and resources of the criminal.

In July 2006, DOJ charged a defendant with 66 counts of false claims to the government, mail fraud, wire fraud, and aggravated identity theft, relating to the defendant's allegedly fraudulent applications for disaster assistance from the Federal Emergency Management Agency (FEMA) following Hurricane Katrina. Using fictitious SSNs and variations of her name, the defendant allegedly received $277,377 from FEMA.

Robert C. Ingardia, a registered representative who had been associated with several broker-dealers, assumed the identity of his customers. Without authorization, Mr. Ingardia changed the address information for their accounts, sold stock in the accounts worth more than $800,000, and, in an effort to manipulate the market for two thinly-traded penny stock companies, used the cash proceeds of the sales to buy more than $230,000 worth of stock in the companies. The SEC obtained a temporary restraining order against Mr. Ingardia in 2001, and a civil injunction against him in 2003 after the United States Attorney's Office for the Southern District of New York obtained a criminal conviction against him in 2002.

III. A Strategy to Combat Identity Theft

Identity theft is a multi-faceted problem for which there is no simple solution. Because identity theft has several stages in its "life cycle," it must be attacked at each of those stages, including:

- when the identity thief attempts to acquire a victim's personal information;
- when the thief attempts to misuse the information he has acquired; and
- after an identity thief has completed his crime and is enjoying the benefits, while the victim is realizing the harm.

The federal government's strategy to combat identity theft must address each of these stages by:

- keeping sensitive consumer data out of the hands of identity thieves in the first place through better data security and by educating consumers on how to protect it;
- making it more difficult for identity thieves, when they are able to obtain consumer data, to use the information to steal identities;
- assisting victims in recovering from the crime; and
- deterring identity theft by aggressively prosecuting and punishing those who commit the crime.

A great deal already is being done to combat identity theft, but there are several areas in which we can improve. The Task Force's recommendations, as described below, are focused on those areas.

A. PREVENTION: KEEPING CONSUMER DATA OUT OF THE HANDS OF CRIMINALS

Identity thieves can ply their trade only if they get access to consumer data. Reducing the opportunities for identity thieves to obtain the data in the first place is the first step to reducing identity theft. Government, the business community, and consumers all play a role in protecting data.

Data compromises can expose consumers to the threat of identity theft or related fraud, damage the reputation of the entity that experienced the breach, and impose the risk of substantial costs for all parties involved. Although there is no such thing as "perfect security," some entities fail to adopt even basic security measures, including many that are inexpensive and readily available.

The link between a data breach and identity theft often is unclear.

Depending on the nature of the breach, the kinds of information breached, and other factors, a particular breach may or may not pose a significant risk of identity theft. Little empirical evidence exists on the extent to which, and under what circumstances, data breaches lead to identity theft, and some studies indicate that data breaches and identity theft may not be strongly linked.[29] Nonetheless, because data thieves search for rich targets of consumer data, it is critical that organizations that collect and maintain sensitive consumer information take reasonable steps to protect it and explore new technologies to prevent data compromises.

1. DECREASING THE UNNECESSARY USE OF SOCIAL SECURITY NUMBERS

The SSN is especially valuable to identity thieves, because often it is the key piece of information used in authenticating the identities of consumers. An identity thief with a victim's SSN and certain other information generally can open accounts or obtain other benefits in the victim's name. As long as SSNs continue to be used for authentication purposes, it is important to prevent thieves from obtaining them.

SSNs are readily available to criminals because they are widely used as consumer identifiers throughout the private and public sectors. Although originally created in 1936 to track workers' earnings for social benefits purposes, use of SSNs has proliferated over ensuing decades. In 1961, the Federal Civil Service Commission established a numerical identification system for all federal employees using the SSN as the identification number. The next year, the IRS decided to begin using the SSN as its taxpayer identification number (TIN) for individuals. Indeed, the use by federal agencies of SSNs for the purposes of employment and taxation, employment verification, and sharing of data for law enforcement purposes, is expressly authorized by statute.

The simplicity and efficiency of using a seemingly unique number that most people already possessed encouraged widespread use of the SSN as an identifier by both government agencies and private enterprises, especially as they adapted their record-keeping and business systems to automated data processing. The use of SSNs is now common in our society.

Employers must collect SSNs for tax reporting purposes. Doctors or hospitals may need them to facilitate Medicare reimbursement. SSNs also are used in internal systems to sort and track information about individuals, and in some cases are displayed on identification cards. In 2004, an estimated 42 million Medicare cards displayed the entire SSN, as did approximately 8 million Department of Defense insurance cards. In addition, although the Veterans Health Administration (VHA) discontinued the issuance of Veterans Identification Cards that display SSNs in March 2004, and has issued new cards that do not display SSNs,

In June 2006, a federal judge in Massachusetts sentenced a defendant to five years in prison after a jury convicted him of passport fraud, SSN fraud, aggravated identity theft, identification document fraud, and furnishing false information to the SSA. The defendant had assumed the identity of a deceased individual and then used fraudulent documents to have the name of the deceased legally changed to a third name. He then used this new name and SSN to obtain a new SSN card, driver's licenses, and United States passport. The case was initiated based on information from the Joint Terrorism Task Force in Springfield, Massachusetts. The agencies involved in the investigation included SSA OIG, Department of State, Massachusetts State Police, and the Springfield and Boston police departments.

In September 2006, a defendant was sentenced by a federal judge in Pennsylvania to six months in prison after pleading guilty to Social Security card misuse and possession of a false immigration document. The defendant provided a fraudulent Permanent Resident Alien card and a fraudulent Social Security card to a state trooper as evidence of authorized stay and employment in the United States. The case was investigated by the SSA's Office of Inspector General (OIG), ICE, and the Pennsylvania State Police.

the VHA estimates that between 3 million and 4 million previously issued cards containing SSNs remain in circulation with veterans receiving VA health care services. Some universities still use the SSN as the students' identification number for a range of purposes, from administering loans to tracking grades, and may place it on students' identification cards, although usage for these purposes is declining.

SSNs also are widely available in public records held by federal agencies, states, local jurisdictions, and courts. As of 2004, 41 states and the District of Columbia, as well as 75 percent of U.S. counties, displayed SSNs in public records.[30] Although the number and type of records in which SSNs are displayed vary greatly across states and counties, SSNs are most often found in court and property records.

No single federal law regulates comprehensively the private sector or government use, display, or disclosure of SSNs; instead, there are a variety of laws governing SSN use in certain sectors or in specific situations. With respect to the private sector, for example, the GLB Act restricts the redisclosure to third parties of non-public personal information, such as SSNs, that was originally obtained from customers of a financial institution; the Health Insurance Portability and Accountability Act (HIPAA) limits covered health care organizations' disclosure of SSNs without patient authorization; and the Driver's Privacy Protection Act prohibits state motor vehicle departments from disclosing SSNs, subject to 14 "permissible uses."[31] In the public sector, the Privacy Act of 1974 requires federal agencies to provide notice to, and obtain consent from, individuals before disclosing their SSNs to third parties, except for an established routine use or pursuant to another Privacy Act exception.[32] A number of state statutes restrict the use and display of SSNs in certain contexts.[33] Even so, a report by the Government Accountability Office (GAO) concluded that, despite these laws, there were gaps in how the use and transfer of SSNs are regulated, and that these gaps create a risk that SSNs will be misused.[34]

There are many necessary or beneficial uses of the SSN. SSNs often are used to match consumers with their records and databases, including their credit files, to provide benefits and detect fraud. Federal, state, and local governments rely extensively on SSNs when administering programs that deliver services and benefits to the public.

Although SSNs sometimes are necessary for legal compliance or to enable disparate organizations to communicate about individuals, other uses are more a matter of convenience or habit. In many cases, for example, it may be unnecessary to use an SSN as an organization's internal identifier or to display it on an identification card. In these cases, a different unique identifier generated by the organization could be equally suitable, but without the risk inherent in the SSN's use as an authenticator.

Some private sector entities and federal agencies have taken steps to reduce unnecessary use of the SSN. For example, with guidance from the SSA OIG, the International Association of Chiefs of Police (IACP) adopted a resolution in September 2005 to end the practice of displaying SSNs in posters and other written materials relating to missing persons. Some health insurance providers also have stopped using SSNs as the subscriber's identification number.[35] Additionally, the Department of Treasury's Financial Management Service no longer includes personal identification numbers on the checks that it issues for benefit payments, federal income tax refund payments, and payments to businesses for goods and services provided to the federal government.

More must be done to eliminate unnecessary uses of SSNs. In particular, it would be optimal to have a unified and effective approach or standard for use or display of SSNs by federal agencies. The Office of Personnel Management (OPM), which issues and uses many of the federal forms and procedures using the SSN, and the Office of Management and Budget (OMB), which oversees the management and administrative practices of federal agencies, can play pivotal roles in restricting the unnecessary use of SSNs, offering guidance on better substitutes that are less valuable to identity thieves, and establishing greater consistency when the use of SSNs is necessary or unavoidable.

When purchasing advertising space in a trade magazine in 2002, a Colorado man wrote his birth date and Social Security number on the payment check. The salesman who received the check then used this information to obtain surgery in the victim's name. Two years later, the victim received a collection notice demanding payment of over $40,000 for the surgery performed on the identity thief. In addition to the damage this caused to his credit rating, the thief's medical information was added to the victim's medical records.

RECOMMENDATION: DECREASE THE UNNECESSARY USE OF SOCIAL SECURITY NUMBERS IN THE PUBLIC SECTOR

To limit the unnecessary use of SSNs in the public sector—and to begin to develop alternative strategies for identity management—the Task Force recommends the following:

- **Complete Review of Use of SSNs.** As recommended in the Task Force's interim recommendations, OPM undertook a review of the use of SSNs in its collection of human resource data from agencies and on OPM-based papers and electronic forms. Based on that review, which OPM completed in 2006, OPM should take steps to eliminate, restrict, or conceal the use of SSNs (including assigning employee identification numbers where practicable), in calendar year 2007. If necessary to implement this recommendation, Executive Order 9397, effective November 23, 1943, which requires federal agencies to use SSNs in "any system of permanent account numbers pertaining to individuals," should be partially rescinded. The use by federal agencies of SSNs for the purposes of employment and taxation, employment verification, and sharing of data for law enforcement purposes, however, is expressly authorized by statute and should continue to be permitted.

- **Issue Guidance on Appropriate Use of SSNs.** Based on its inventory, OPM should issue policy guidance to the federal human capital management community on the appropriate and inappropriate use of SSNs in employee records, including the appropriate way to restrict, conceal, or mask SSNs in employee records and human resource management information systems. OPM should issue this policy in calendar year 2007.

- **Require Agencies to Review Use of SSNs.** OMB has surveyed all federal agencies regarding their use of SSNs to determine the circumstances under which such use can be eliminated, restricted, or concealed in agency business processes, systems, and paper and electronic forms, other than those authorized or approved by OPM. OMB should complete the analysis of these surveys in the second quarter of 2007.[36]

- **Establish a Clearinghouse for Agency Practices that Minimize Use of SSNs.** Based on results from OMB's review of agency practices on the use of SSNs, the SSA should develop a clearinghouse for agency practices and initiatives that minimize use and display of SSNs to facilitate sharing of best practices—including the development of any alternative strategies for identity management—to avoid duplication of effort, and to promote interagency collaboration in the development of more effective measures. This should be accomplished by the fourth quarter of 2007.

- **Work with State and Local Governments to Review Use of SSNs.** In the second quarter of 2007, the Task Force should begin to work with state and local governments—through organizations such as the National Governor's Association, the National Association of Attorneys General, the National League of Cities, the National Association of Counties, the U.S. Conference of Mayors, the National District Attorneys Association, and the National Association for Public Health Statistics and Information Systems—to highlight and discuss the vulnerabilities created by the use of SSNs and to explore ways to eliminate unnecessary use and display of SSNs.

RECOMMENDATION: DEVELOP COMPREHENSIVE RECORD ON PRIVATE SECTOR USE OF SSNs

SSNs are an integral part of our financial system. They are essential in matching consumers to their credit file, and thus essential in granting credit and detecting fraud, but their availability to identity thieves creates a possibility of harm to consumers. Beginning in 2007, the Task Force should develop a comprehensive record on the uses of the SSN in the private sector and evaluate their necessity. Specifically, the Task Force member agencies that have direct experience with the private sector use of SSNs, such as DOJ, FTC, SSA, and the financial regulatory agencies, should gather information from stakeholders—including the financial services industry, law enforcement agencies, the consumer reporting agencies, academics, and consumer advocates. The Task Force should then make recommendations to the President as to whether additional specific steps should be taken with respect to the use of SSNs. Any such recommendations should be made to the President by the first quarter of 2008.

2. DATA SECURITY IN THE PUBLIC SECTOR

While private organizations maintain consumer information for commercial purposes, public entities, including federal agencies, collect personal information about individuals for a variety of purposes, such as determining program eligibility and delivering efficient and effective services. Because this information often can be used to commit identity theft, agencies must guard against unauthorized disclosure or misuse of personal information.

a. Safeguarding of Information in the Public Sector

Two sets of laws and associated policies frame the federal government's responsibilities in the area of data security. The first specifically governs the federal government's information privacy program, and includes such laws as the Privacy Act, the Computer Matching and Privacy Protection Act, and provisions of the E-Government Act.[37] The other concerns the information and information technology security program. The Federal Information Security Management Act (FISMA), the primary governing statute for this program, establishes a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets, and provides for development and maintenance of minimum controls required to protect federal information and information systems. FISMA assigns specific policy and oversight responsibilities to OMB, technical guidance responsibilities to the National Institute of Standards and Technology (NIST), implementation responsibilities to all agencies, and an operational assistance role to the Department of Homeland Security (DHS). FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. It further requires agency operational program officials, Chief Information Officers (CIOs), and Inspectors General (IGs) to conduct annual reviews of the agency information security program and report the results to OMB. Additionally, as part of its oversight role, OMB issued several guidance memoranda last year on how agencies should safeguard sensitive information, including a memorandum addressing FISMA oversight and reporting, and which provided a checklist developed by NIST concerning protection of remotely accessed information, and that recommended that agencies, among other things, encrypt all data on mobile devices and use a "time-out" function for remote access and mobile devices.[38] The United States Computer Emergency Readiness Team (US-CERT) has also played an important role in public sector data security.[39]

Federal law also requires that agencies prepare extensive data collection analyses and report periodically to OMB and Congress. The President's Management Agenda (PMA) requires agencies to report quarterly to OMB on selected performance criteria for both privacy and security. Agency performance levels for both status and progress are graded on a PMA Scorecard.[40]

Federal agency performance on information security has been uneven. As a result, OMB and the agencies have undertaken a number of initiatives to improve the government security programs. OMB and DHS are leading an interagency Information Systems Security Line of Business (ISS LOB) working group, exploring ways to improve government data security practices. This effort already has identified a number of key areas for improving government-wide security programs and making them more cost-effective.

Employee training is essential to the effectiveness of agency security programs. Existing training programs must be reviewed continuously and updated to reflect the most recent changes, issues, and trends. This effort includes the development of annual general security awareness training for all government employees using a common curriculum; recommended security training curricula for all employees with significant security responsibilities; an information-sharing repository/portal of training programs; and opportunities for knowledge-sharing (e.g., conferences and seminars). Each of these components builds elements of agency security awareness and practices, leading to enhanced protection of sensitive data.

b. Responding to Data Breaches in the Public Sector

Several federal government agencies suffered high-profile security breaches involving sensitive personal information in 2006. As is true with private sector breaches, the loss or compromise of sensitive personal information by the government has made affected individuals feel exposed and vulnerable and may increase the risk of identity theft. Until this Task Force issued guidance on this topic in September 2006, government agencies had no comprehensive formal guidance on how to respond to data breaches, and in particular, had no guidance on what factors to consider in deciding (1) whether a particular breach warrants notice to consumers, (2) the content of the notice, (3) which third parties, if any, should be notified, and (4) whether to offer affected individuals credit monitoring or other services.

The experience of the last year also has made one thing apparent: an agency that suffers a breach sometimes faces impediments in its ability to effectively respond to the breach by notifying persons and entities in a position to cooperate (either by assisting in informing affected individuals or by actively preventing or minimizing harms from the breach). For example, an agency that has lost data such as bank account numbers might want to share that information with the appropriate financial institutions, which could assist in monitoring for bank fraud and in identifying the account holders for possible notification. The very information that may be most necessary to disclose to such persons and entities, however, often will be information maintained by federal agencies that is subject to the Privacy Act. Critically, the Privacy Act prohibits the disclosure of any record in a system of records unless the subject individual has given written consent or unless the disclosure falls within one of 12 statutory exceptions.

RECOMMENDATION: EDUCATE FEDERAL AGENCIES ON HOW TO PROTECT THEIR DATA AND MONITOR COMPLIANCE WITH EXISTING GUIDANCE

To ensure that government agencies receive specific guidance on concrete steps that they can take to improve their data security measures, the Task Force recommends the following:

- **Develop Concrete Guidance and Best Practices.** OMB and DHS, through the current interagency Information Systems Security Line of Business (ISS LOB) task force, should (a) outline best practices in the area of automated tools, training, processes, and standards that would enable agencies to improve their security and privacy programs, and (b) develop a list of the most common 10 or 20 “mistakes” to avoid in protecting information held by the government. The Task Force made this recommendation as part of its interim recommendations to the President, and it should be implemented and completed in the second quarter of 2007.
- **Comply With Data Security Guidance.** OMB already has issued an array of data security regulations and standards aimed at urging agencies to better protect their data. Given that data breaches continue to occur, however, it is imperative that agencies continue to report compliance with its data security guidelines and

directives to OMB. If any agency does not comply fully, OMB should note that fact in the agency's quarterly PMA Scorecard.

- **Protect Portable Storage and Communications Devices.** Many of the most publicized data breaches in recent months involved losses of laptop computers. Because government employees increasingly rely on laptops and other portable communications devices to conduct government business, no later than the second quarter of 2007, all Chief Information Officers of federal agencies should remind the agencies of their responsibilities to protect laptops and other portable data storage and communication devices. If any agency does not fully comply, that failure should be reflected on the agency's PMA scorecard.

RECOMMENDATION: ENSURE EFFECTIVE, RISK-BASED RESPONSES TO DATA BREACHES SUFFERED BY FEDERAL AGENCIES

To assist agencies in responding to the difficult questions that arise following a data breach, the Task Force recommends the following:

- **Issue Data Breach Guidance to Agencies.** The Task Force developed and formally approved a set of guidelines, reproduced in Appendix A, that sets forth the factors that should be considered in deciding whether, how, and when to inform affected individuals of the loss of personal data that can contribute to identity theft, and whether to offer services such as free credit monitoring to the persons affected. In the interim recommendations, the Task Force recommended that OMB issue that guidance to all agencies and departments. OMB issued the guidance on September 20, 2006.

- **Publish a "Routine Use" Allowing Disclosure of Information Following a Breach.** To allow agencies to respond quickly to data breaches, including by sharing information about potentially affected individuals with other agencies and entities that can assist in the response, federal agencies should, in accordance with the Privacy Act exceptions, publish a routine use that specifically permits the disclosure of information in connection with response and remediation efforts in the event of a data breach. Such a routine use would serve to protect the interests of the people whose information is at risk by allowing agencies to take appropriate steps to facilitate a timely and effective response, thereby improving their ability to prevent, minimize, or remedy any harms that may result from a compromise of data maintained in their systems of records. This routine use should not affect the existing ability of agencies to properly disclose and share information for law enforcement purposes. The Task Force offers the routine use that is reproduced in Appendix B as a model for other federal agencies to use in developing and publishing their own routine uses.[41] DOJ has now published such a routine use, which became effective as of January 24, 2007. The proposed routine use language reproduced in Appendix B should be reviewed and adapted by agencies to fit their individual systems of records.

3. DATA SECURITY IN THE PRIVATE SECTOR

Data protection in the private sector is the subject of numerous legal requirements, industry standards and guidelines, private contractual arrangements, and consumer and business education initiatives. But no system is perfect, and data breaches can occur even when entities have implemented appropriate data safeguards.

a. The Current Legal Landscape

Although there is no generally applicable federal law or regulation that protects all consumer information or requires that such information be secured, a variety of specific statutes and regulations impose data security requirements for particular entities in certain contexts. These include Title V of the GLB Act, and its implementing rules and guidance, which require financial institutions to maintain reasonable protections for the personal information they collect from customers [42]; Section 5 of the FTC Act, which prohibits unfair or deceptive practices [43]; the FCRA,[44] which restricts access to consumer reports and imposes safe disposal requirements, among other things [45]; HIPAA, which protects health information [46]; Section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act,[47] which requires verification of the identity of persons opening accounts with financial institutions; and the Drivers Privacy Protection Act of 1994 (DPPA), which prohibits most disclosures of drivers' personal information.[48] See Volume II, Part A, for a description of federal laws and regulations related to data security.

The federal bank regulatory agencies—the Federal Deposit Insurance Corporation (FDIC), Federal Reserve Board (FRB), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS)—and the FTC and SEC, among others, have pursued active regulatory and enforcement programs to address the data security practices of those entities within their respective jurisdictions. Depending on the severity of a violation, the financial regulatory agencies have cited institutions for violations, without taking formal action when management quickly remedied the situation.

BJ's Wholesale Club, Inc. suffered a data breach that led to the loss of thousands of credit card numbers and millions of dollars in unauthorized charges. Following the breach, the FTC charged the company with engaging in an unfair practice by failing to provide reasonable security for credit card information. The FTC charged that BJ's stored the information in unencrypted clear text without a business need to do so, failed to defend its wireless systems against unauthorized access, failed to use strong credentials to limit access to the information, and failed to use adequate procedures for detecting and investigating intrusions. The FTC also charged that these failures were easy to exploit by hackers, and led to millions of dollars in fraudulent charges.

In circumstances where the situation was not quickly remedied, the financial regulatory agencies have taken formal, public actions and sought civil penalties, restitution, and cease and desist orders. The FDIC has taken 17 formal enforcement actions between the beginning of 2002 and the end of 2006; the FRB has taken 14 formal enforcement actions since 2001; the OCC has taken 18 formal actions since 2002; and the OTS has taken eight formal enforcement actions in the past five years. Remedies in these cases have included substantial penalties and restitution, consumer notification, and restrictions on the use of customer information. Additionally, the FTC has obtained orders against 14 companies that allegedly failed to implement reasonable procedures to safeguard the sensitive consumer information they maintained. Most of these cases have been brought in the last two years. The SEC also has brought data security cases. See Volume II, Part B, for a description of enforcement actions relating to data security.

In April 2004, the New York Attorney General settled a case with Barnes&Noble.com, fining the company $60,000 and requiring it to implement a data security program after an investigation revealed that an alleged design vulnerability in the company's website permitted unauthorized access to consumers' personal information and enabled thieves to make fraudulent purchases. In addition, California, Vermont, and New York settled a joint action with Ziff Davis Media, Inc. involving security shortcomings that exposed the credit card numbers and other personal information of about 12,000 consumers.

In addition to federal law, every state and the District of Columbia has its own laws to protect consumers from unfair or deceptive practices. Moreover, 37 states have data breach notice laws,[49] and some states have laws relevant to data security, including safeguards and disposal requirements.

Trade associations, industry collaborations, independent organizations with expertise in data security, and nonprofits have developed guidance and standards for businesses. Topics include: incorporating basic security and privacy practices into everyday business operations; developing privacy and security plans; employee screening, training, and management; implementing electronic and physical safeguards; employing threat recognition techniques; safeguarding international transactions; and credit and debit card security.[50]

Some entities that use service providers also have begun using contractual provisions that require third-party service vendors with access to the institution's sensitive data to safeguard that data.[51] Generally, these provisions also address specific practices for contracting organizations, including conducting initial and follow-up security audits of a vendor's data center, and requiring vendors to provide certification that they are in compliance with the contracting organization's privacy and data protection obligations.[52]

In 2006, the Federal Reserve Board issued a Cease and Desist Order against an Alabama-based financial institution for, among other things, failing to comply with an existing Board regulation that required implementation of an information security program.

b. Implementation of Data Security Guidelines and Rules

Many private sector organizations understand their vulnerabilities and have made significant strides in incorporating data security into their operations or improving existing security programs. See Volume II, Part C, for a description of education efforts for businesses on safeguarding data. For example, many companies and financial institutions now regularly require two-factor authentication for business conducted via computer or telephone; send dual confirmations when customers submit a change of address; limit access to non-public personal information to necessary personnel; regularly monitor websites for phishing and firewalls for hacking; perform assessments of network security to determine the adequacy of protection from intrusion, viruses, and other data security breaches; and post identity theft education materials on company websites. Additionally, many firms within the consumer data industry offer services that provide companies with comprehensive background checks on prospective employees and tenants as permitted by law under the FCRA, and help companies verify the identity of customers.

Yet, as the reports of data breach incidents continue to show, further improvements are necessary. In a survey of financial institutions, 95 percent of respondents reported growth in their information security budget in 2005, with 71 percent reporting that they have a defined information security governance framework.[53] But many organizations also report that they are in the early stages of implementing comprehensive security procedures. For instance, in a survey of technology decision makers released in 2006, 85 percent of respondents indicated that their stored data was either somewhat or extremely vulnerable, while only 22 percent had implemented a storage security solution to prevent unauthorized access.[54] The same survey revealed that 58 percent of data managers responding believed their networks were not as secure as they could be.[55]

Small businesses face particular challenges in implementing effective data security policies for reasons of cost and lack of expertise. A 2005 survey found that while many small businesses are accelerating their adoption and use of information technology and the Internet, many do not have basic security measures in place.[56] For example, of the small businesses surveyed,

- nearly 20 percent did not use virus scans for email, a basic information security safeguard;
- over 60 percent did not protect their wireless networks with even the simplest of encryption solutions;
- over 70 percent reported expectations of a more challenging environment for detecting security threats, but only 30 percent reported increasing information security spending in 2005; and
- 74 percent reported having no information security plan in place.

Further complicating matters is the fact that some federal agencies are unable to receive data from private sector entities in an encrypted form. Therefore, some private sector entities that have to transmit sensitive data to federal agencies—sometimes pursuant to law or regulations issued by agencies—are unable to fully safeguard the transmitted data because they must decrypt the data before they can send it to the agencies. The

In 2005, the FTC settled a law enforcement action with Superior Mortgage, a mortgage company, alleging that the company failed to comply with the GLB Safeguards Rule. The FTC alleged that the company's security procedures were deficient in the areas of risk assessment, access controls, document protection, and oversight of service providers. The FTC also charged Superior with misrepresenting how it applied encryption to sensitive consumer information. Superior agreed to undertake a comprehensive data security program and retain an independent auditor to assess and certify its security procedures every two years for the next 10 years.

In 2004, an FDIC examination of a state-chartered bank disclosed significant computer system deficiencies and inadequate controls to prevent unauthorized access to customer information. The FDIC issued an order directing the bank to develop and implement an information security program, and specifically ordered the bank, among other things, to perform a formal risk assessment of internal and external threats that could result in unauthorized access to customer information. The bank also was ordered to review computer user access levels to ensure that access was restricted to only those individuals with a legitimate business need to access the information.

E-Authentication Presidential Initiative is currently addressing how agencies can more uniformly adopt appropriate technical solutions to this problem based on the level of risk involved, including, but not limited to, encryption.

c. Responding to Data Breaches in the Private Sector

Although the link between data breaches and identity theft is unclear, reports of private sector data security breaches add to consumers' fear of identity thieves gaining access to sensitive consumer information and undermine consumer confidence. Pursuant to the GLB Act, the financial regulatory agencies require financial institutions under their jurisdiction to implement programs designed to safeguard customer information. In addition, the federal bank regulatory agencies (FDIC, FRB, NCUA, OCC, and OTS) have issued guidance with respect to breach notification. In addition, 37 states have laws requiring that consumers be notified when their information has been subject to a breach.[57] Some of the laws also require that the entity that experienced the breach notify law enforcement, consumer reporting agencies, and other potentially affected parties.[58] Notice to consumers may help them avoid or mitigate injury by allowing them to take appropriate protective actions, such as placing a fraud alert on their credit file or monitoring their accounts. In some cases, the organization experiencing the breach has offered additional assistance, including free credit monitoring services. Moreover, prompt notification to law enforcement allows for the investigation and deterrence of identity theft and related unlawful conduct.

The states have taken a variety of approaches regarding when notice to consumers is required. Some states require notice to consumers whenever there is unauthorized access to sensitive data. Other states require notification only when the breach of information poses a risk to consumers. Notice is not required, for example, when the data cannot be used to commit identity theft, or when technological protections prevent fraudsters from accessing data. This approach recognizes that excessive breach notification can overwhelm consumers, causing them to ignore more significant incidents, and can impose unnecessary costs on consumers, the organization that suffered the breach, and others. Under this approach, however, organizations struggle to assess whether the risks are sufficient to warrant consumer notification. Factors relevant to that assessment often include the sensitivity of the breached information, the extent to which it is protected from access (e.g., by using technological tools for protecting data), how the breach occurred (e.g., whether the information was deliberately stolen as opposed to accidentally misplaced), and any evidence that the data actually have been misused.

A number of bills establishing a federal notice requirement have been introduced in Congress. Many of the state laws and the bills in Congress address who should be notified, when notice should be given, what information should be provided in the notice, how notice should be effected, and the circumstances under which consumer notice should be delayed for law enforcement purposes.

Despite the substantial effort undertaken by the public and private sectors to educate businesses on how to respond to data breaches (see Volume II, Part D, for a description of education for businesses on responding to data breaches), there is room for improvement by businesses in planning for and responding to data breaches. Surveys of large corporations and retailers indicate that fewer than half of them have formal breach response plans. For example, an April 2006 cross-industry survey revealed that only 45 percent of large multinational corporations headquartered in the U.S. had a formal process for handling security violations and data breaches.[59] Fourteen percent of the companies surveyed had experienced a significant privacy breach in the past three years.[60] A July 2005 survey of large North American corporations found that although 80 percent of responding companies reported having privacy or data-protection strategies, only 31 percent had a formal notification procedure in the event of a data breach.[61] Moreover, one survey found that only 43 percent of retailers had formal incident response plans, and even fewer had tested their plans.[62]

When an online retailer became the target of an elaborate fraud ring, the company looked to one of the major credit reporting agencies for assistance. By using shared data maintained by that agency, the retailer was able to identify applications with common data elements and flag them for further scrutiny. By using the shared application data in connection with the activities of this fraud ring, the company avoided $26,000 in fraud losses.

RECOMMENDATION: ESTABLISH NATIONAL STANDARDS EXTENDING DATA PROTECTION SAFEGUARDS REQUIREMENTS AND BREACH NOTIFICATION REQUIREMENTS

Several existing laws mandate protection for sensitive consumer information, but a number of private entities are not subject to those laws. The GLB Act, for example, applies to "financial institutions," but generally not to other entities that collect and maintain sensitive information. Similarly, existing federal breach notification standards do not extend to all entities that hold sensitive consumer information, and the various state laws that contain breach notification requirements differ in various respects, complicating compliance. Accordingly, the Task Force recommends the development of (1) a national standard imposing safeguards requirements on all private entities that maintain sensitive consumer information; and (2) a national standard requiring entities that maintain sensitive consumer information to provide notice to consumers and law enforcement in the event of a breach. Such national standards should provide clarity and predictability for businesses and consumers, and should incorporate the following important principles.

Covered data. The national standards for data security and for breach notification should cover data that can be used to perpetrate identity theft—in particular, any data or combination of consumer data that would allow someone to use, log into, or access an individual's account, or to establish a new account using the individual's identifying information. This identifying information includes a name, address, or telephone number paired with a unique identifier such as a Social Security number, a driver's license number, a biometric record, or a financial account number (together with a PIN or security code, if such PIN or code is required to access an account) (hereinafter "covered data"). The standards should not cover data, such as a name and address alone, that by itself typically would not cause harm. The definitions of covered data for data security and data breach notification requirements should be consistent.

Covered entities. The national standards for data security and breach notification should cover any private entity that collects, maintains, sells, transfers, disposes of, or otherwise handles covered data in any medium, including electronic and paper formats.

Unusable data. National standards should recognize that rendering data unusable to outside parties likely would prevent "acquisition" of the data, and thus ordinarily would satisfy an entity's legal obligations to protect the data and would not trigger notification of a breach. The standards should not endorse a specific technology because unusability is not a static concept and the effectiveness of particular technologies may change over time.

Risk-based standard for breach notification. The national breach notification standard should require that covered entities provide notice to consumers in the event of a data breach, but only when the risks to consumers are real—that is, when there is a significant risk of identity theft due to the breach. This "significant risk of identity theft" trigger for notification recognizes that excessive breach notification can overwhelm consumers, causing them to take costly actions when there is little risk, or conversely, to ignore the notices when the risks are real.

Notification to law enforcement. The national breach notification standard should provide for timely notification to law enforcement and expressly allow law enforcement to authorize a delay in required consumer notice, either for law enforcement or national security reasons (and either on its own behalf or on behalf of state or local law enforcement).

Relationship to current federal standards. The national standards for data security and breach notification should be drafted to be consistent with and so as not to displace any rules, regulations, guidelines, standards, or guidance issued under the GLB Act by the FTC, the federal bank regulatory agencies, the SEC, or the Commodity Futures Trading Commission (CFTC), unless those agencies so determine.

Preemption of state laws. To ensure comprehensive national requirements that provide clarity and predictability, while maintaining an effective enforcement role for the states, the national data security and breach notification standards should preempt state data security and breach notification laws, but authorize enforcement by the state Attorneys General for entities not subject to the jurisdiction of the federal bank regulatory agencies, the SEC, or the CFTC.

Rulemaking and enforcement authority. Coordinated rulemaking authority under the Administrative Procedure Act should be given to the FTC, the federal bank regulatory agencies, the SEC, and the CFTC to implement the national standards. Those agencies should be authorized to enforce the standards against entities under their respective jurisdictions, and should specifically be authorized to seek civil penalties in federal district court.

Private right of action. The national standards should not provide for or create a private right of action.

Standards incorporating such principles will prompt covered entities to establish and implement administrative, technical, and physical safeguards to ensure the security and confidentiality of sensitive consumer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer. Because the costs associated with implementing safeguards or providing breach notice may be different for small businesses and larger businesses, or may differ based on the type of information held by a business, the national standard should expressly call for actions that are *reasonable* for the particular covered entity and should not adopt a one-size-fits-all approach to the implementation of safeguards.

When a major consumer lending institution encountered a problem when the loss ratio on many of its loans —including mortgages and consumer loans—became excessively high due to fraud, the bank hired a leading provider of fraud prevention products to authenticate potential customers during the application process prior to extending credit. The result was immediate: two million dollars of confirmed fraud losses were averted within the first six months of implementation.

RECOMMENDATION: BETTER EDUCATE THE PRIVATE SECTOR ON SAFEGUARDING DATA

Although much has been done to educate the private sector on how to safeguard data, the continued proliferation of data breaches suggests that more needs to be done. While there is no perfect data security system, a company that is sensitized to the

A leading payment processing and bill payment company recently deployed an automated fraud detection and case management system to more than 40 financial institutions. The system helps ensure that receiving and paying bills online remains a safe practice for consumers. To mitigate risk and reduce fraud for banks and consumers before it happens, the system combines the company's cumulative knowledge of payment patterns and a sophisticated analytics engine to help financial services organizations detect and stop unauthorized payments.

importance of data security, understands its legal obligations, and has the information it needs to secure its data adequately, is less likely to suffer a data compromise. The Task Force therefore makes the following recommendations concerning how to better educate the private sector:

- **Hold Regional Seminars for Businesses on Safeguarding Information.** By the fourth quarter of 2007, the federal financial regulatory agencies and the FTC, with support from other Task Force member agencies, should hold regional seminars and develop self-guided and online tutorials for businesses and financial institutions, about safeguarding information, preventing and reporting breaches, and assisting identity theft victims. The seminar's leaders should make efforts to include small businesses in these sessions and address their particular needs. These seminars could be co-sponsored by local bar associations, the Better Business Bureaus (BBBs), and other similar organizations. Self-guided tutorials should be made available through the Task Force's online clearinghouse at ***www.idtheft.gov***.
- **Distribute Improved Guidance for Private Industry.** In the second quarter of 2007, the FTC should expand written guidance to private sector entities that are not regulated by the federal bank regulatory agencies or the SEC on steps they should take to safeguard information. The guidance should be designed to give a more detailed explanation of the broad principles encompassed in existing laws. Like the Information Technology Examination Handbook's Information Security Booklet issued under the auspices of the Federal Financial Institutions Examination Council,[63] the guidance should be risk-based and flexible, in recognition of the fact that different private sector entities will warrant different solutions.

RECOMMENDATION: INITIATE INVESTIGATIONS OF DATA SECURITY VIOLATIONS

Beginning immediately, appropriate government agencies should initiate investigations of and, if appropriate, take enforcement actions against entities that violate the laws governing data security. The FTC, SEC, and federal bank regulatory agencies have used regulatory and enforcement efforts to require companies to maintain appropriate information safeguards under the law. Federal agencies should continue and expand these efforts to ensure that such entities use reasonable data security measures. Where appropriate, the agencies should share information about those enforcement actions on ***www.idtheft.gov***.

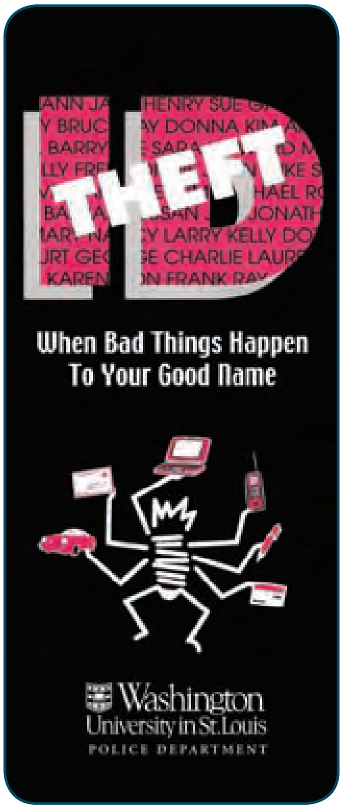
4. EDUCATING CONSUMERS ON PROTECTING THEIR PERSONAL INFORMATION

The first line of defense against identity theft often is an aware and motivated consumer who takes reasonable precautions to protect his information. Every day, unwitting consumers create risks to the security of their personal information. From failing to install firewall protection on a computer hard drive to leaving paid bills in a mail slot, consumers leave the door open to identity thieves. Consumer education is a critical component of any plan to reduce the incidence of identity theft.

The federal government has been a leading provider of consumer information about identity theft. Numerous departments and agencies target identity theft-related messages to relevant populations. *See* Volume II, Part E, for a description of federal consumer education efforts. The FTC, through its Identity Theft Clearinghouse and ongoing outreach, plays a primary role in consumer awareness and education, developing information that has been co-branded by a variety of groups and agencies. Its website, ***www.ftc.gov/idtheft*** serves as a comprehensive one-stop resource in both English and Spanish for consumers. The FTC also recently implemented a national public awareness campaign centered around the themes of "Deter, Detect, and Defend," which seeks to drive behavioral changes in consumers that will reduce their risk of identity theft (Deter); encourage them to monitor their credit reports and accounts to alert them of identity theft as soon as possible after it occurs (Detect); and mitigate the damage caused by identity theft should it occur (Defend). This campaign, mandated in the FACT Act, consists of direct messaging to consumers as well as material written for organizations, community leaders, and local law enforcement. The Deter, Detect, and Defend materials have been adopted and distributed by hundreds of entities, both public and private.

The SSA and the federal regulatory agencies are among the many other government bodies that also play a significant role in educating consumers on how to protect themselves. For example, the SSA added a message to its SSN verification printout warning the public not to share their SSNs with others. This warning was especially timely in the aftermath of Hurricane Katrina, which necessitated the issuance of a large number of those printouts. Similarly, the Senior Medicare Patrol (SMP) program, funded by U.S. Administration on Aging in the Department of Health and Human Services, uses senior volunteers to educate their peers about protecting their personal information and preventing and identifying consumer and health care fraud. The SMP program also has worked closely with the Centers for Medicare and Medicaid Services to protect seniors from new scams aimed at defrauding them of their Medicare numbers and other personal information. And the U.S. Postal Inspection Service has produced a number of consumer education materials, including several videos, alerting the public to the problems associated with identity theft.

Significant consumer education efforts also are taking place at the state level. Nearly all of the state Attorneys General offer information on the prevention and remediation of identity theft on their websites, and several states have conducted conferences and workshops focused on education and training in privacy protection and identity theft prevention. Over the past year, the Attorney General of Illinois and the Governors of New Mexico and California have hosted summit meetings, bringing together law enforcement, educators, victims' coordinators, consumer advocates, and the business community to develop better strategies for educating the public and fighting identity theft. The National Governors Association convened the National Strategic Policy Council on Cyber and Electronic Crime in September 2006 to trigger a coordinated education and prevention effort by federal, state, and local policymakers. The New York State Consumer Protection Board has conducted "Consumer Action Days," with free seminars about identity theft and other consumer protection issues.



Police departments also provide consumer education to their communities. Many departments have developed materials and make them available in police stations, in city government buildings, and on websites.[64] As of this writing, more than 500 local police departments are using the FTC's "Deter, Detect, Defend" campaign materials to teach their communities about identity theft. Other groups, including the National Apartment Association and the National Association of Realtors, also have promoted this campaign by distributing the materials to their membership.

Although most educational material is directed at consumers in general, some is aimed at and tailored to specific target groups. One such group is college students. For several reasons—including the vast amounts of personal data that colleges maintain about them and their tendency to keep personal data unguarded in shared dormitory rooms—students are frequent targets of identity thieves. According to one report, one-third to one-half of all reported personal information breaches in 2006 have occurred at colleges and universities.[65] In recognition of the increased vulnerability of this population, many universities are providing information to their students about the risks of identity theft through web sites, orientation campaigns, and seminars.[66]

Federal, state, and local government agencies provide a great deal of identity theft-related information to the public through the Internet, printed materials, DVDs, and in-person presentations. The messages the agencies provide—how to protect personal information, how to recognize a potential problem, where to report a theft, and how to deal with the aftermath—are echoed by industry, law enforcement, advocates, and the media. See Volume II, Part F, for a description of private sector consumer education efforts. But there is little coordination among the agencies on current education programs. Dissemination in some cases is random, information is limited, and evaluation of effectiveness is almost nonexistent. Although a great deal of useful information is being disseminated, the extent to which the messages are reaching, engaging, or motivating consumers is unclear.

RECOMMENDATION: INITIATE A MULTI-YEAR PUBLIC AWARENESS CAMPAIGN

Because consumer education is a critical component of any plan to reduce the incidence of identity theft, the Task Force recommends that member agencies, in the third quarter of 2007, initiate a multi-year national public awareness campaign that builds on the FTC's current "AvoID Theft: Deter, Detect, Defend" campaign, developed pursuant to direction in the FACT Act. This campaign should include the following elements:

- **Develop a Broad Awareness Campaign.** By broadening the current FTC campaign into a multi-year awareness campaign, and by engaging the Ad Council or similar entities as partners, important and empowering messages should be disseminated more widely and by more partners. The campaign should include public service announcements on the Internet, radio, and television, and in newspapers and magazines, and should address the issue from a variety of perspectives, from prevention through mitigation and remediation, and reach a variety of audiences.
- **Enlist Outreach Partners.** The agencies conducting the campaign should enlist as outreach partners national organizations either that have been active in helping consumers protect themselves against identity theft, such as the AARP, the Identity Theft Resource Center (ITRC), and the Privacy Rights Clearinghouse (PRC), or that may be well-situated to help in this area, such as the White House Office of Faith-Based and Community Initiatives.
- **Increase Outreach to Traditionally Underserved Communities.** Outreach to underserved communities should include encouraging language translations of existing materials and involving community-based organizations as partners.
- **Establish "Protect Your Identity Days."** The campaign should establish "Protect Your Identity Days" to promote better data security by businesses and individual commitment to security by consumers. These "Protect Your Identity Days" should also build on the popularity of community "shred-ins" by encouraging community and business organizations to shred documents containing personal information.

RECOMMENDATION: DEVELOP AN ONLINE CLEARINGHOUSE" FOR CURRENT EDUCATIONAL RESOURCES

The Task Force recommends that in the third quarter of 2007, the Task Force member agencies develop an online "clearinghouse" for current identity theft educational resources for consumers, businesses, and law enforcement from a variety of sources at ***www.idtheft.gov***. This would make the materials immediately available in one place to any public or private entity willing to launch an education program, and to any citizen interested in accessing the information. Rather than recreate content, entities could link directly to the clearinghouse for timely and accurate information. Educational materials should be added to the website on an ongoing basis.

B. PREVENTION: MAKING IT HARDER TO MISUSE CONSUMER DATA

Keeping valuable consumer data out of the hands of criminals is the first step in reducing the incidence of identity theft. But, because no security is perfect and thieves are resourceful, it is essential to reduce the opportunities for criminals to misuse the data they do manage to steal.

An identity thief who wants to open new accounts in a victim's name must be able to (1) provide identifying information to enable the creditor or other grantor of benefits to access information on which to base an eligibility decision, and (2) convince the creditor or other grantor of benefits that he is, in fact, the person he purports to be. For example, a credit card grantor processing an application for a credit card will use the SSN to access the consumer's credit report to check his creditworthiness, and may rely on photo documents, the SSN, and/or other proof to access other sources of information intended to "verify" the applicant's identity. Thus, the SSN is a critical piece of information for the thief, and its wide availability increases the risk of identity theft.

Identity systems follow a two-fold process: first, determining ("identification") and setting ("enrollment") the identity of an individual at the onset of the relationship; and second, later ensuring that the individual is the same person who was initially enrolled ("authentication"). With the exception of banks, savings associations, credit unions, some broker-dealers, mutual funds, futures commission merchants, and introducing brokers (collectively, "financial institutions"), there is no generally-applicable legal obligation on private sector entities to use any particular means of identification. Financial institutions are required to follow certain verification procedures pursuant to regulations promulgated by the federal bank regulatory agencies, the Department of

Treasury, the SEC, and the CFTC under the USA PATRIOT Act.[67] The regulations require these financial institutions to establish a Customer Identification Program (CIP) specifying identifying information that will be obtained from each customer when accounts are opened (which must include, at a minimum, name, date of birth, address, and an identification number such as an SSN). The CIP requirement is intended to ensure that financial institutions form a reasonable belief that they know the true identity of each customer who opens an account. The government, too, is making efforts to implement new identification mechanisms. For example, REAL ID is a nationwide effort intended to prevent terrorism, reduce fraud, and improve the reliability and accuracy of identification documents that state governments issue.[68] See Volume II, Part G, for a description of recent laws relating to identification documents.

The verification process can fail, however, in a number of ways. First, identity documents may be falsified. Second, checking the identifying information against other verifying sources of information can produce varying results, depending on the accuracy of the initial information presented and the accuracy or quality of the verifying sources. The process also can fail because employees are trained improperly or fail to follow proper procedures. Identity thieves exploit each of these opportunities to circumvent the verification process.[69]

Once an individual's identity has been verified, it must be authenticated each time he wants the access for which he was initially verified, such as access to a bank account. Generally, businesses authenticate an individual by requiring him to present some sort of credential to prove that he is the same individual whose identity was originally verified. A credential is generally one or more of the following:

- Something a person knows—most commonly a password, but also may be a query that requires specific knowledge only the customer is likely to have, such as the exact amount of the customer's monthly mortgage payment.
- Something a person has—most commonly a physical device, such as a Universal Serial Bus (USB) token, a smart card, or a password-generating device.[70]
- Something a person is—most commonly a physical characteristic, such as a fingerprint, iris, face, and hand geometry. This type of authentication is referred to as biometrics.[71]

Some entities use a single form of authentication—most commonly a password—but if it is compromised, there are no other fail-safes in the system. To address this problem, the federal bank regulatory agencies issued guidance promoting stronger customer authentication methods for certain high-risk transactions. Such methods are to include the use of multi-factor authentication, layered security, or other similar controls reasonably calculated to mitigate the exposure from any transactions that are identified as high-risk. The guidance more broadly provides that banks, savings associations, and credit unions conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing Internet-based financial services.[72] Financial institutions covered by the guidance were advised that the agencies expected them to have completed the risk assessment and implemented risk mitigation activities by year-end 2006.[73] Along with the financial services industry, other industries have begun to implement new authentication procedures using different types of credentials.

SSNs have many advantages and are widely used in our current marketplace to match consumers with their records (including their credit files) and as part of the authentication process. Keeping the authentication process convenient for consumers and credit grantors without making it too easy for criminals to impersonate consumers requires a fine balance. Notwithstanding improvements in certain industries and companies, efforts to facilitate the development of better ways to authenticate consumers without undue burden would help prevent criminals from profiting from their crime.

▶ RECOMMENDATION: HOLD WORKSHOPS ON AUTHENTICATION

Because developing more reliable methods of authenticating the identities of individuals would make it harder for identity thieves to open new accounts or access existing accounts using other individuals' information, the Task Force will hold a workshop or series of workshops, involving academics, industry, and entrepreneurs, focused on developing and promoting improved means of authenticating the identities of individuals. These experts will discuss the existing problem and examine the limitations of current processes of authentication. With that information, the Task Force will probe viable technological and other solutions that will reduce identity fraud, and identify needs for future research. Such workshops have been successful in developing creative and timely responses to consumer protection issues, and the workshops are expected to be useful for both the private and public sectors. For example, the federal government has an interest as a facilitator of the development of new technologies and in implementing technologies that better protect the data it handles in providing benefits and services, and as an employer.

As noted in the Task Force's interim recommendations to the President, the FTC and other Task Force member agencies will host the first such workshop in the second quarter of 2007. The Task Force also recommends that a report be issued or subsequent workshops be held to report on any proposals or best practices identified during the workshop series.

RECOMMENDATION: DEVELOP COMPREHENSIVE RECORD ON PRIVATE SECTOR USE OF SSNs

As noted in Section III A 1, above, the Task Force recommends developing a comprehensive record on the uses of the SSN in the private sector and evaluating their necessity.

C. VICTIM RECOVERY: HELPING CONSUMERS REPAIR THEIR LIVES

Because identity theft can be committed despite the best of precautions, an essential step in the fight against this crime is ensuring that victims have the knowledge, tools, and assistance necessary to minimize the damage and begin the recovery process. Currently, consumers have a number of rights and available resources, but they may not be aware of them.

1. VICTIM ASSISTANCE: OUTREACH AND EDUCATION

Federal and state laws offer victims of identity theft an array of tools to avoid or mitigate the harms they suffer. For example, under the FACT Act, victims can: (1) place alerts on their credit files; (2) request copies of applications and other documents used by the thief; (3) request that the credit reporting agencies block fraudulent trade lines on credit reports; and (4) obtain information on the fraudulent accounts from debt collectors.

In some cases, the recovery process is relatively straightforward. Consumers whose credit card numbers have been used to make unauthorized purchases, for example, typically can get the charges removed without undue burden. In other cases, however, such as those involving new-account fraud, recovery can be an ordeal.

Widely-available guidance advises consumers of steps to take if they have become victims of identity theft, or if their personal information has been breached. For example, the FTC's website, ***www.ftc.gov/idtheft***, contains step-by-step recovery information for victims, as well as for those who may be at risk following a compromise of their data. Many other agencies and organizations link directly to the FTC site and themselves provide education and assistance to victims.

Fair and Accurate Credit Transaction Act (FACT Act) Rights

The Fair and Accurate Credit Transactions Act of 2003 added new sections to the Fair Credit Reporting Act that provide a number of new tools for victims to recover from identity theft. These include the right to place a fraud alert with the credit reporting agencies and receive a free copy of the credit report. An initial alert lasts for 90 days. A victim with an identity theft report documenting actual misuse of the consumer information is entitled to place a 7-year alert on his file. In addition, under the FACT Act, victims can request copies of documents relating to fraudulent transactions, and can obtain information from a debt collector regarding a debt fraudulently incurred in the victim's name. Victims who have a police report also can ask that fraudulent accounts be blocked from their credit report, and can prevent businesses from reporting information that resulted from identity theft to the credit reporting agencies.

Identity theft victims, and consumers who suspect that they may become victims because of lost data, are advised to act quickly to prevent or minimize harm. The steps are straightforward:

- *Contact one of the three major credit reporting agencies to place a fraud alert on their credit file. The agencies are required to transmit this information to the other two companies. Consumers who place this 90-day alert are entitled to a free copy of their credit report. Fraud alerts are most useful when a consumer's SSN is compromised, creating the risk of new account fraud.*

- *Contact any creditors where fraudulent accounts were opened or charges were made to dispute these transactions, and follow up in writing.*

- *Report actual incidents of identity theft to the local police department and obtain a copy of the police report. This document will be essential to exercising other remedies.*

- *Report the identity theft incident to the ID Theft Data Clearinghouse by filing a complaint online at ftc.gov/idtheft, or calling toll free 877 ID THEFT. The complaint will be entered into the Clearinghouse and shared with the law enforcement agencies who use the database to investigate and prosecute identity crimes.*

- *Some states provide additional protections to identity theft victims by allowing them to request a "credit freeze," which prevents consumers' credit reports from being released without their express consent. Because most companies obtain a credit report from a consumer before extending credit, a credit freeze will likely prevent the extension of credit in a consumer's name without the consumer's express permission.*

State governments also provide assistance to victims. State consumer protection agencies, privacy agencies, and state Attorneys General provide victim information and guidance on their websites, and some provide personal assistance as well. A number of states have established hotlines, counseling, and other assistance for victims of identity theft. For example, the Illinois Attorney General's office has implemented an Identity Theft Hotline; each caller is assigned a consumer advocate to assist with the recovery process and to help prevent further victimization.

A number of private sector organizations also provide critical victim assistance. Not-for-profit groups such as the Privacy Rights Clearinghouse (PRC) and the Identity Theft Resource Center (ITRC) offer counseling and assistance for identity theft victims who need help in going through the recovery process. The Identity Theft Assistance Center (ITAC), a victim assistance program established by the financial services industry, has helped approximately 13,000 victims resolve problems with disputed accounts and other fraud related to identity theft since its founding in 2004. Finally, many individual companies have established hotlines, distributed materials, and provided special services for customers whose information has been misused. Indeed, some companies rely on their identity theft services as marketing tools.

Despite this substantial effort by the public and private sectors to educate and assist victims, there is room for improvement. Many victims are not aware, or do not take advantage, of the resources available to them. For example, while the FTC receives roughly 250,000 contacts from victims every year, that number is only a small percentage of all identity theft victims. Moreover, although first responders could be a key resource for identity theft victims, the first responders often are overworked and may not have the information that they need about the steps for victim recovery. It is essential, therefore, that public and private outreach efforts be expanded, better coordinated, and better funded.

▶ RECOMMENDATION: PROVIDE SPECIALIZED TRAINING ABOUT VICTIM RECOVERY TO FIRST RESPONDERS AND OTHERS PROVIDING DIRECT ASSISTANCE TO IDENTITY THEFT VICTIMS

First responders and others who provide direct assistance and support to identity theft victims must be adequately trained. Accordingly, the Task Force recommends the following:

- **Train Local Law Enforcement Officers.** By the third quarter of 2007, federal law enforcement agencies, which could include the U.S. Postal Inspection Service, the FBI, the Secret Service, and the FTC, should conduct training seminars—delivered in person, online, or via video—for local law enforcement officers on available resources and providing assistance for victims.
- **Provide Educational Materials for First Responders That Can Be Readily Used as a Reference Guide for Identity Theft Victims.** During the third quarter of 2007, the FTC and DOJ should develop a reference guide, which should include contact information for resources and information on first steps to recovery, and should make that guide available to law enforcement officers through the online clearinghouse at

www.idtheft.gov. Such guidance would assist first responders in directing victims on their way to recovery.

- **Distribute an Identity Theft Victim Statement of Rights.** Federal law provides substantial assistance to victims of identity theft. From obtaining a police report to blocking fraudulent accounts in a credit report, consumers—as well as law enforcement, private businesses, and other parties involved in the recovery process—need to know what remedies are available. Accordingly, the Task Force recommends that, during the third quarter of 2007, the FTC draft an ID Theft Victim Statement of Rights, a short and simple statement of the basic rights victims possess under current law. This document should then be disseminated to victims through law enforcement, the financial sector, and advocacy groups, and posted at ***www.idtheft.gov***.

- **Develop Nationwide Training for Victim Assistance Counselors.** Crime victims receive assistance through a wide array of federal and state-sponsored programs, as well as nonprofit organizations. Additionally, every United States Attorney's Office in the country has a victim-witness coordinator who is responsible for referring crime victims to the appropriate resources to resolve harms that resulted from the misuse of their information. All of these counselors should be trained to respond to the specific needs of identity theft victims, including assisting them in coping with the financial and emotional impact of identity crime. Therefore, the Task Force recommends that a standardized training curriculum for victim assistance be developed and promoted through a nationwide training campaign, including through DOJ's Office for Victims of Crime (OVC). Already, OVC has begun organizing training workshops, the first of which was held in December 2006. These workshops are intended to train not only victim-witness coordinators from U.S. Attorney's Offices, but also state, tribal, and local victim service providers. The program will help advocates learn how to assist victims in self-advocacy and how and when to intervene in a victim's recovery process. Training topics will include helping victims deal with the economic and emotional ramifications of identity theft, assisting victims with understanding how an identity theft case proceeds through the criminal justice system, and identity theft laws. Additional workshops should be held in 2007.

RECOMMENDATION: DEVELOP AVENUES FOR INDIVIDUALIZED ASSISTANCE TO IDENTITY THEFT VICTIMS

Although many victims are able to resolve their identity theft-related issues without assistance, some individuals would benefit from individualized counseling. The availability of personalized assistance should be increased through national service organizations, such as those using retired seniors or similar groups, and pro bono activities by lawyers, such as those organized by the American Bar Association (ABA). In offering individualized assistance to identity theft victims, these organizations and programs should use the victim resource guides that are already available through the FTC and DOJ's Office for Victims of Crime. Specifically, the Task Force also recommends the following:

- **Engage the American Bar Association to Develop a Program Focusing on Assisting Identity Theft Victims with Recovery.** The ABA has expertise in coordinating legal representation in specific areas of practice through law firm volunteers. Moreover, law firms have the resources and expertise to staff an effort to assist victims of identity theft. Accordingly, the Task Force recommends that, beginning in 2007, the ABA, with assistance from the Department of Justice, develop a pro bono referral program focusing on assisting identity theft victims with recovery.

2. MAKING IDENTITY THEFT VICTIMS WHOLE

Identity theft inflicts many kinds of harm upon its victims, making it difficult for them to feel that they ever will recover fully. Beyond tangible forms of harm, statistics cannot adequately convey the emotional toll that identity theft often exacts on its victims, who frequently report feelings of violation, anger, anxiety, betrayal of trust, and even self-blame or hopelessness. These feelings may continue, or even increase, as victims work through the credit recovery and criminal justice processes. Embarrassment, cultural factors, or personal or family circumstances (e.g., if the victim has a relationship to the identity thief) may keep the victims from reporting the problem to law enforcement, in turn making them ineligible to take advantage of certain remedies. Often, these reactions are intensified by the ongoing, long-term nature of the crime. Criminals may not stop committing identity theft after having been caught; they simply use information against the same individual in a new way, or they sell the information so that multiple identity thieves can use it. Even when the fraudulent activity ceases, the effects of negative information on the victim's credit report can continue for years.

The many hours victims spend in attempting to recover from the harms they suffer often takes a toll on victims that is not reflected in their monetary losses. One reason that identity theft can be so destructive to its victims is the sheer amount of time and energy often required to recover from the offense, including having to correct credit reports, dispute charges with individual creditors, close and reopen bank accounts, and monitor credit reports for future problems arising from the theft.

> "I received delinquent bills for purchases she [the suspect] made. I spent countless hours on calls with creditors in Texas who were reluctant to believe that the accounts that had been opened were fraudulent. I spent days talking to police in Texas in an effort to convince them that I was allowed by Texas law to file a report and have her [the suspect] charged with the theft of my identity.... I had to send more than 50 letters to the creditors to have them remove the more than 60 inquiries that were made by this woman...."
>
> Nicole Robinson
> Testimony before
> House Ways and
> Means Committee,
> Subcommittee on
> Social Security
> May 22, 2001

In addition to losing time and money, some identity theft victims suffer the indignity of being mistaken for the criminal who stole their identities, and have been wrongfully arrested.[74] In one case, a victim's driver's license was stolen, and the information from the license was used to open a fraudulent bank account and to write more than $10,000 in bad checks. The victim herself was arrested when local authorities thought she was the criminal. In addition to the resulting feelings of trauma, this type of harm is a particularly difficult one for an identity theft victim to resolve.

▶ RECOMMENDATION: AMEND CRIMINAL RESTITUTION STATUTES TO ENSURE THAT VICTIMS RECOVER FOR THE VALUE OF TIME SPENT IN ATTEMPTING TO REMEDIATE THE HARMS THEY SUFFERED

Restitution to victims from convicted thieves is available for the direct financial costs of identity theft offenses. However, there is no specific provision in the federal restitution statutes for compensation for the time spent by victims recovering from the crime, and court decisions interpreting the statutes suggest that such recovery would be precluded.

As stated in the Task Force's interim recommendations to the President, the Task Force recommends that Congress amend the federal criminal restitution statutes to allow for restitution from a criminal defendant to an identity theft victim, in an amount equal to the value of the victim's time reasonably spent attempting to remediate the intended or actual harm incurred from the identity theft offense. The language of the proposed amendment is in Appendix C. DOJ transmitted the proposed amendment to Congress on October 4, 2006.

▶ RECOMMENDATION: EXPLORE THE DEVELOPMENT OF A NATIONAL PROGRAM ALLOWING IDENTITY THEFT VICTIMS TO OBTAIN AN IDENTIFICATION DOCUMENT FOR AUTHENTICATION PURPOSES

One of the problems faced by identity theft victims is proving that they are who they say they are. Indeed, some identity theft victims have been mistaken for the criminal who stole their identity, and have been arrested based on warrants issued for the thief who stole their personal data. To give identity theft victims a means to authenticate their identities in such a situation, several states have developed identification documents, or "passports," that authenticate identity theft victims. These voluntary mechanisms are designed to prevent the misuse of the victim's name in the criminal justice system when, for example, an identity thief uses his victim's name when arrested. These documents often use multiple factors for authentication, such as biometric data and a password. The FBI has established a similar system through the National Crime Information Center, allowing identity theft victims to place their name in an "Identity File." This program, too, is limited in scope. Beginning in 2007, the Task Force member agencies should lead an effort to study the feasibility of developing a nationwide system allowing identity theft victims to obtain a document that they can use to avoid being mistaken for the suspect who has misused their identity. The system should build on the programs already used by several states and the FBI.

3. GATHERING BETTER INFORMATION ON THE EFFECTIVENESS OF VICTIM RECOVERY MEASURES

Identity theft victims have been granted many new rights in recent years. Gathering reliable information about the utility of these new rights is critical to evaluating whether they are working well or need to be modified. Additionally, because some states have measures in place to assist identity theft victims that have no federal counterpart, it is important to assess the success of those measures to determine whether they should be adopted more widely. Building a record of victims' experiences in exercising their rights is therefore crucial to ensuring that any strategy to fight identity theft is well-supported.

RECOMMENDATION: ASSESS EFFICACY OF TOOLS AVAILABLE TO VICTIMS

The Task Force recommends the following surveys or assessments:

- **Conduct Assessment of FACT Act Remedies Under FCRA.** The FCRA is among the federal laws that enable victims to restore their good name. The FACT Act amendments to the FCRA provide several new rights and tools for actual or potential identity theft victims, including the availability of credit file fraud alerts; the blocking of fraudulent trade lines on credit reports; the right to have creditors cease furnishing information relating to fraudulent accounts to credit reporting agencies; and the right to obtain business records relating to fraudulent accounts. Many of these rights have been in effect for a short time. Accordingly, the Task Force recommends that the agencies with enforcement authority for these statutory provisions assess their impact and effectiveness through appropriate surveys. Agencies should report on the results in calendar year 2008.

- **Conduct Assessment of State Credit Freeze Laws.** Among the state-enacted remedies without a federal counterpart is one granting consumers the right to obtain a credit freeze. Credit freezes make a consumer's credit report inaccessible when, for example, an identity thief attempts to open an account in the victim's name. State laws differ in several respects, including whether all consumers can obtain a freeze or only identity theft victims; whether credit reporting agencies can charge the consumer for unfreezing a file (which would be necessary when applying for credit); and the time allowed to the credit reporting agencies to unfreeze a file. These provisions are relatively new, and there is no "track record" to show how effective they are, what costs they may impose on consumers and businesses, and what features are most beneficial to consumers. An assessment of how these measures have been implemented and how effective they have been would help policy makers in considering whether a federal credit freeze law would be appropriate. Accordingly, the Task Force recommends that the FTC, with support from the Task Force member agencies, assess the impact and effectiveness of credit freeze laws, and report on the results in the first quarter of 2008.

D. LAW ENFORCEMENT: PROSECUTING AND PUNISHING IDENTITY THIEVES

The two keys to preventing identity theft are (1) preventing access to sensitive consumer information through better data security and increased education, and (2) preventing the misuse of information that may be obtained by would-be identity thieves. Should those mechanisms fail, strong criminal law enforcement is necessary to both punish and deter identity thieves.

The increased awareness about identity theft in recent years has made it necessary for many law enforcement agencies at all levels of government to devote additional resources to investigating identity theft-related crimes. The principal federal law enforcement agencies that investigate identity theft are the FBI, the United States Secret Service, the United States Postal Inspection Service, SSA OIG, and ICE. Other agencies, as well as other federal Inspectors General, also may become involved in identity theft investigations.

In investigating identity theft, law enforcement agencies use a wide range of techniques, from physical surveillance to financial analysis to computer forensics. Identity theft investigations are labor-intensive, and because no single investigator can possess all of the skill sets needed to handle each of these functions, the investigations often require multiple detectives, analysts, and agents. In addition, when a suspected identity

In September 2006, the Michigan Attorney General won the conviction of a prison inmate who had orchestrated an elaborate scheme to claim tax refunds owed to low income renters through the state's homestead property tax program. Using thousands of identities, the defendant and his cohorts were detected by alert U.S. Postal carriers who were suspicious of the large number of Treasury checks mailed to certain addresses.

theft involves large numbers of potential victims, investigative agencies may need additional personnel to handle victim-witness coordination and information issues.

During the last several years, federal and state agencies have aggressively enforced the laws that prohibit the theft of identities. All 50 states and the District of Columbia have some form of legislation that prohibits identity theft, and in all those jurisdictions, except Maine, identity theft can be a felony. See Volume II, Part H, for a description of state criminal law enforcement efforts. In the federal system, a wide range of statutory provisions is used to investigate and prosecute identity theft including, most notably, the aggravated identity theft statute[75] enacted in 2004, which carries a mandatory two-year prison sentence. Since then, DOJ has made increasing use of the aggravated identity theft statute: in Fiscal Year 2006, DOJ charged 507 defendants with aggravated identity theft, up from 226 defendants charged with aggravated identity theft in Fiscal Year 2005. In many of these cases, the courts have imposed substantial sentences. See Volume II, Part I, for a description of sentencing in federal identity theft prosecutions.

The Department of Justice also has initiated many special identity theft initiatives in recent years. The first of these, in May 2002, involved 73 criminal prosecutions by U.S. Attorney's Offices against 135 individuals in 24 federal districts. Since then, identity theft has played an integral part in several initiatives that DOJ and other agencies have directed at online economic crime. For example, "Operation Cyber Sweep," a November 2003 initiative targeting Internet-related economic crime, resulted in the arrest or conviction of more than 125 individuals and the return of indictments against more than 70 people involved in various types of Internet-related fraud and economic crime. See Volume II, Part J, for a description of special enforcement and prosecution initiatives.

In a "Operation Firewall," the Secret Service was responsible for the first-ever takedown of a large illegal online bazaar. Using the website www.shadowcrew.com, the Shadowcrew organization had thousands of members engaged in the online trafficking of stolen identity information and documents, such as drivers' licenses, passports, and Social Security cards, as well as stolen credit card, debit card, and bank account numbers. The Shadowcrew members trafficked in at least 1.7 million stolen credit card numbers and caused total losses in excess of $4 million. The Secret Service successfully shut down the website following a year-long undercover investigation, which resulted in the arrests of 21 individuals in the United States on criminal charges in October 2004. Additionally, law enforcement officers in six foreign countries arrested or searched eight individuals.

1. COORDINATION AND INTELLIGENCE/INFORMATION SHARING

Federal law enforcement agencies have recognized the importance of coordination among agencies and of information sharing between law enforcement and the private sector. Coordination has been challenging, however, for several reasons: identity theft data currently reside in numerous databases; there is no standard reporting form for all identity theft complaints; and many law enforcement agencies have limited resources. Given these challenges, law enforcement has responded to the need for greater cooperation by, among other things, forming interagency task forces and developing formal intelligence-sharing mechanisms. Law enforcement also has worked to develop methods of facilitating the timely receipt and analysis of identity theft complaint data and other intelligence.

a. Sources of Identity Theft Information

Currently, federal law enforcement has a number of sources of information about identity theft. The primary source of direct consumer complaint data is the FTC, which, through its Identity Theft Clearinghouse, makes available to law enforcement through a secure website the complaints it receives. Internet-related identity theft complaints also are received by the Internet Crime Complaint Center (IC3), a joint venture of the FBI and National White Collar Crime Center. The IC3 develops case leads from the complaints it receives and sends them to law enforcement throughout the country. Additionally, a special component of the FBI that works closely with the IC3 is the Cyber Initiative and Resource Fusion Unit (CIRFU). The CIRFU, based in Pittsburgh, facilitates the operation of the National Cyber Forensic Training Alliance (NCFTA), a public/private alliance and fusion center, by maximizing intelligence development and analytical resources from law enforcement and critical industry partners. The U.S. Postal Inspection Service also hosts its Financial Crimes Database, a web-based national database available to U.S. Postal Service inspectors for use in analyzing mail theft and identity theft complaints received from various sources. These are but a few of the sources of identity theft data for law enforcement. See Volume II, Part K, for a description of how law enforcement obtains and analyzes identity theft data.

Private sector entities—including the financial services industry and credit reporting agencies—also are important sources of identity theft information for law enforcement agencies. They often are best positioned to identify early anomalies in various components of the e-commerce environment in which their businesses interact, which may represent the earliest indicators of an identity theft scenario. For this reason and others, federal law enforcement has undertaken numerous public- and private-sector collaborations in recent years to improve information sharing. For example, corporations have placed analysts and investigators with IC3 in support of initiatives and investigations. In addition, ITAC, the cooperative initiative of the financial services industry, shares information with law enforcement and the FTC to help catch and convict the criminals responsible for identity theft. See Volume II, Part K, for a description of other private sector sources of identity theft data. Such alliances enable critical industry experts and law enforcement agencies to work together to more expeditiously receive and process information and intelligence vital both to early identification of identity theft schemes and rapid development of aggressive investigations and mitigation strategies, such as public service advisories. At the same time, however, law enforcement agencies report that they have encountered obstacles in obtaining support and assistance from key private-sector stakeholders in some cases, absent legal process, such as subpoenas, to obtain information.

One barrier to more complete coordination is that identity theft information resides in multiple databases, even within individual law enforcement agencies. A single instance of identity theft may result in information being posted at federal, state, and local law enforcement agencies, credit reporting agencies, credit issuers, financial institutions, telecommunications companies, and regulatory agencies. This, in turn, leads to the inefficient "stove-piping" of relevant data and intelligence. Additionally, in many cases, agencies do not or cannot share information with other agencies, making it difficult to determine whether an identity theft complaint is related to a single incident or a series of incidents. This problem may be even more pronounced at the state and local levels.

b. Format for Sharing Information and Intelligence

A related issue is the inability of the primary law enforcement agencies to communicate electronically using a standard format, which greatly impedes the sharing of criminal law enforcement information. When data collection systems use different formats to describe the same event or fact, at least one of the systems must be reprogrammed to fit the other program's terms. Where several hundred variables are involved, the programming resources required to connect the two databases can be an insurmountable barrier to data exchange.

To address that concern, several law enforcement organizations, including the International Association of Chiefs of Police's (IACP) Private Sector Liaison Committee and the Major Cities' Chiefs (MCC), have recommended developing a standard electronic identity theft police report form. Reports that use a standard format could be shared among law enforcement agencies and stored in a national repository for investigatory purposes.

c. Mechanisms for Sharing Information

Law enforcement uses a variety of mechanisms to facilitate information sharing and intelligence analysis in identity-theft investigations. See Volume II, Part L, for a description of federal law enforcement outreach efforts. As just one example, the Regional Information Sharing Systems (RISS) Program is a long-standing, federally-funded program to support regional law enforcement efforts to combat identity theft and other crimes. Within that program, law enforcement has established intelligence-sharing systems. These include, for example, the Regional Identity Theft Network (RITNET), created to provide Internet-accessible identity theft information for federal, state, and local law enforcement agencies within the Eastern District of Pennsylvania. RITNET is designed to include data from the FTC, law enforcement agencies, and the banking industry, and allow investigators to connect crimes committed in various jurisdictions and link investigators. It also will collect information on all reported frauds, regardless of size, thereby eliminating the advantage identity thieves have in keeping theft amounts low.

Multi-agency working groups and task forces are another successful investigative approach, allowing different agencies to marshal resources, share intelligence, and coordinate activities. Federal authorities lead or co-lead over 90 task forces and working groups devoted (in whole or in part) to identity theft. See Volume II, Part M, for a description of interagency working groups and task forces.

Despite these efforts, coordination among agencies can be improved. Better coordination would help law enforcement officers "connect the dots" in investigations and pool limited resources.

RECOMMENDATION: ESTABLISH A NATIONAL IDENTITY THEFT LAW ENFORCEMENT CENTER

The Task Force recommends that the federal government establish, as resources permit, an interagency National Identity Theft Law Enforcement Center to better consolidate, analyze, and share identity theft information among law enforcement agencies, regulatory agencies, and the private sector. This effort should be led by the Department of Justice and include representatives of federal law enforcement agencies, including the FBI, the Secret Service, the U.S. Postal Inspection Service, the SSA OIG, and the FTC. Leveraging existing resources, increased emphasis should be placed on the analysis of identity theft complaint data and other information and intelligence related to identity theft from public and private sources, including from identity theft investigations. This information should be made available to appropriate law enforcement at all levels to aid in the investigation, prosecution, and prevention of identity theft crimes, including to target organized groups of identity thieves and the most serious offenders operating both in the United States and abroad. Effective mechanisms that enable law enforcement officers from around the country to share, access, and search appropriate law enforcement information around-the-clock, including through remote access, should also be developed. As an example, intelligence from documents seized during investigations could help facilitate the ability of agents and officers to "connect the dots" between various investigations around the country.

In a case prosecuted by the United States Attorney's Office for the Eastern District of Pennsylvania, a gang purchased 180 properties using false or stolen names. The thieves colluded to procure inflated appraisals for the properties, obtained financing, and drained the excess profits for their own benefit, resulting in harm to the identity theft victims and to the neighborhood when most of the properties went into foreclosure.

RECOMMENDATION: DEVELOP AND PROMOTE THE ACCEPTANCE OF A UNIVERSAL IDENTITY THEFT REPORT FORM

The Task Force recommended in its interim recommendations that the federal government, led by the FTC, develop and promote a universal police report like that recommended by the IACP and MCC—a standard document that an identity theft victim could complete, print, and take to any local law enforcement agency for verification and incorporation into the police department's report system. This would make it easier for victims to obtain these reports, facilitate entry of the information into a central database that could be used by law enforcement to analyze patterns and trends, and initiate more investigations of identity theft.

Criminal law enforcers, the FTC, and representatives of financial institutions, the consumer data industry, and consumer advocacy groups have worked together to develop a standard form that meets this need and captures essential information. The resulting Identity Theft Complaint ("Complaint") form was made available in October 2006 via the FTC's Identity Theft website, *www.ftc.gov/idtheft*. Consumers can print copies of their completed Complaint and take it to their police station, where it can be used as the basis for a police report. The Complaint provides much greater specificity about the details of the crime than would a typical police report, so consumers will be able to submit it to credit reporting agencies and creditors to assist in resolving their identity theft-related problems. Further, the information they enter into the Complaint will be collected in the FTC's Identity Theft Data Clearinghouse, thus enriching this source of consumer complaints for law enforcement. This system also relieves the burden on local law enforcement because consumers are completing the detailed Complaint before filing their police report.

RECOMMENDATION: ENHANCE INFORMATION SHARING BETWEEN LAW ENFORCEMENT AND THE PRIVATE SECTOR

Because the private sector in general, and financial institutions in particular, are an important source of identity theft-related information for law enforcement, the Task Force recommends the following steps to enhance information sharing between law enforcement and the private sector:

- **Enhance Ability of Law Enforcement to Receive Information From Financial Institutions.** Section 609(e) of the Fair Credit Reporting Act enables identity theft victims to receive identity theft-related documents and to designate law enforcement agencies to receive the documents on their behalf. Despite that fact, law enforcement agencies have sometimes encountered difficulties in obtaining such information without a subpoena. By the second quarter of 2007, DOJ should initiate discussions with the financial sector to ensure greater compliance with this law, and should include other law enforcement agencies in these discussions. DOJ, on an ongoing basis, should compile any recommendations that may result from those discussions and, where appropriate, relay those recommendations to the appropriate private or public sector entity for action.

- **Initiate Discussions With the Financial Services Industry on Countermeasures to Identity Thieves.** Federal law enforcement agencies, led by the U.S. Postal Inspection Service, should continue discussions with the financial services industry as early as the second quarter of 2007 to develop more effective fraud prevention measures to deter identity thieves who acquire data through mail theft. Discussions should include use of the Postal Inspection Service's current Financial Industry Mail Security Initiative. The Postal Inspection Service, on an ongoing basis, should compile any recommendations that may result from those discussions and, where appropriate, relay those recommendations to the appropriate private or public sector entity for action.

- **Initiate Discussions With Credit Reporting Agencies On Preventing Identity Theft.** By the second quarter of 2007, DOJ should initiate discussions with the credit reporting agencies on possible measures that would make it more difficult for identity thieves to obtain credit based on access to a victim's credit report. The discussions should include other law enforcement agencies, including the FTC. DOJ, on an ongoing basis, should compile any recommendations that may result from the discussions and, where appropriate, relay the recommendations to the appropriate private or public sector entity for action.

2. COORDINATION WITH FOREIGN LAW ENFORCEMENT

Federal enforcement agencies have found that a significant portion of the identity theft committed in the United States originates in other countries. Therefore, coordination and cooperation with foreign law enforcement is essential. A positive step by the United States in ensuring such coordination was the ratification of the Convention on Cybercrime (2001). The Cybercrime Convention is the first multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks, including offenses that relate to the stealing of personal information and the exploitation of that information to commit fraud. The Cybercrime Convention requires parties to establish laws against these offenses, to ensure that domestic laws give law enforcement officials the necessary legal authority to gather electronic evidence, and to provide international cooperation to other parties in the fight against computer-related crime. The United States participated in the drafting of the Convention and, in November 2001, was an early signatory.

Because of the international nature of many forms of identity theft, providing assistance to, and receiving assistance from, foreign law enforcement on identity theft is critical for U.S. enforcement agencies. Under current law, the United States generally is able to provide such assistance, which fulfills our obligations under various treaties and enhances our ability to obtain reciprocal assistance from foreign agencies. Indeed, there are numerous examples of collaborations between U.S. and foreign law enforcement in identity theft investigations.

Nevertheless, law enforcement faces several impediments in their ability to coordinate efforts with foreign counterparts. First, even though federal law enforcement agencies have successfully identified numerous foreign suspects trafficking in stolen consumer information, their ability to arrest and prosecute these criminals is very limited. Many countries do not have laws directly addressing identity theft, or have general fraud laws that do not parallel those in the United States. Thus, investigators in the United States may be able to prove violations of American identity theft statutes, yet be unable to show violations of the foreign country's law. This can impact cooperation on extradition or collection of evidence necessary to prosecute offenders in the United States. Additionally, some foreign governments are unwilling to cooperate fully with American law enforcement representatives, or may cooperate but fail to aggressively prosecute offenders or seize criminal assets.

Second, certain statutes governing foreign requests for electronic and other evidence—specifically, 18 U.S.C. § 2703 and 28 U.S.C. § 1782—fail to make clear whether, how, and in which court certain requests can be fulfilled. This jurisdictional uncertainty has impeded the ability of American law enforcement officers to assist their counterparts in other countries who are conducting identity theft investigations.

The FBI Legal Attache in Bucharest recently contributed to the development and launch of **www.efrauda.ro**, a Romanian government website for the collection of fraud complaints based on the IC3 model. The IC3 also provided this Legal Attache with complaints received by U.S. victims who were targets of a Romanian Internet crime ring. The complaint forms provided to Romanian authorities via the Legal Attache assisted the Romanian police and Ministry of Justice with the prosecution of Romanian subjects.

RECOMMENDATION: ENCOURAGE OTHER COUNTRIES TO ENACT SUITABLE DOMESTIC LEGISLATION CRIMINALIZING IDENTITY THEFT

The Department of Justice, after consulting with the Department of State, should formally encourage other countries to enact suitable domestic legislation criminalizing identity theft. A number of countries already have adopted, or are considering adopting, criminal identity-theft offenses. In addition, since 2005, the United Nations Crime Commission (UNCC) has convened an international Expert Group to examine the worldwide problem of fraud and identity theft. That Expert Group is drafting a report to the UNCC (for presentation in 2007) that is expected to describe the major trends in fraud and identity theft in numerous countries and to offer recommendations on best practices by governments and the private sector to combat fraud and identity theft. DOJ should provide input to the Expert Group concerning the need for the criminalization of identity theft worldwide.

RECOMMENDATION: FACILITATE INVESTIGATION AND PROSECUTION OF INTERNATIONAL IDENTITY THEFT BY ENCOURAGING OTHER NATIONS TO ACCEDE TO THE CONVENTION ON CYBERCRIME, OR TO ENSURE THAT THEIR LAWS AND PROCEDURES ARE AT LEAST AS COMPREHENSIVE

Global acceptance of the Convention on Cybercrime will help to assure that all countries have the legal authority to collect electronic evidence and the ability to cooperate in trans-border identity theft investigations that involve electronic data. The U.S. government should continue its efforts to promote universal accession to the Convention and assist other countries in bringing their laws into compliance with the Convention's standards. The Department of State, in close coordination with the Department of Justice and Department of Homeland Security, should lead this effort through appropriate bilateral and multilateral outreach mechanisms. Other agencies, including the Department of Commerce and the FTC, should participate in these outreach efforts as appropriate. This outreach effort began years ago in a number of international settings, and should continue until broad international acceptance of the Convention on Cybercrime is achieved.

RECOMMENDATION: IDENTIFY COUNTRIES THAT HAVE BECOME SAFE HAVENS FOR PERPETRATORS OF IDENTITY THEFT AND TARGET THEM FOR DIPLOMATIC AND ENFORCEMENT INITIATIVES FORMULATED TO CHANGE THEIR PRACTICES.

Safe havens for perpetrators of identity theft and individuals who aid and abet such illegal activities should not exist. However, the inaction of law enforcement agencies in some countries has turned those countries into breeding grounds for sophisticated criminal networks devoted to identity theft. Countries that tolerate the existence of such criminal networks encourage their growth and embolden perpetrators to expand their operations. In 2007, the U.S. law enforcement community, with input from the international law enforcement community, should identify the countries that are safe havens for identity thieves. Once identified, the U.S. government should use appropriate diplomatic measures and any suitable enforcement mechanisms to encourage those countries to change their practices.

RECOMMENDATION: ENHANCE THE U.S. GOVERNMENT'S ABILITY TO RESPOND TO APPROPRIATE FOREIGN REQUESTS FOR EVIDENCE IN CRIMINAL CASES INVOLVING IDENTITY THEFT

The Task Force recommends that Congress clarify which courts can respond to appropriate foreign requests for electronic and other evidence in criminal investigations, so that the United States can better provide prompt assistance to foreign law enforcement in identity theft cases. This clarification can be accomplished by amending 18 U.S.C. § 2703 and making accompanying amendments to 18 U.S.C. §§ 2711 and 3127, and by enacting a new statute, 18 U.S.C. § 3512, which would supplement the foreign assistance authority of 28 U.S.C. § 1782. Proposed language for these legislative changes is available in Appendix D (text of amendments to 18 U.S.C. §§ 2703, 2711, and 3127, and text of new language for 18 U.S.C. § 3512).

RECOMMENDATION: ASSIST, TRAIN, AND SUPPORT FOREIGN LAW ENFORCEMENT

Because the investigation of major identity theft rings increasingly will require foreign cooperation, federal law enforcement agencies, led by DOJ, FBI, Secret Service, USPIS, and ICE, should assist, train, and support foreign law enforcement through the use of Internet intelligence-collection entities, including IC3 and CIRFU, and continue to make it a priority to work with other countries in joint investigations targeting identity theft. This work should begin in the third quarter of 2007.

3. PROSECUTION APPROACHES AND INITIATIVES

As part of its effort to prosecute identity theft aggressively, DOJ, since 2002, has conducted a number of enforcement initiatives that have focused, in whole or in part, on identity theft. In addition to broader enforcement initiatives led by DOJ, various individual U.S. Attorney's Offices have undertaken their own identity theft efforts. For example, the U.S. Attorney's Office in the District of Oregon has an identity theft "fast track" program that requires eligible defendants to plead guilty to aggravated identity theft and agree, without litigation, to a 24-month minimum mandatory sentence. Under this program, it is contemplated that defendants will plead guilty and be sentenced on the same day, without the need for a pre-sentence report to be completed prior to the guilty plea, and waive all appellate and post-conviction remedies. In exchange for their pleas of guilty, defendants are not charged with the predicate offense, such as bank fraud or mail theft, which would otherwise result in a consecutive sentence under the United States Sentencing Guidelines. In addition, two U.S. Attorney's Offices have collaborated on a special initiative to combat passport fraud, known as Operation Checkmate. See Volume II, Part J.

Notwithstanding these efforts, challenges remain for federal law enforcement. Because of limited resources and a shortage of prosecutors, many U.S. Attorney's Offices have monetary thresholds—i.e., requirements that a certain amount of monetary loss must have been suffered by the victims—before the U.S. Attorney's Office will open an identity theft case. When a U.S. Attorney's Office declines to open a case based on a monetary threshold, investigative agents cannot obtain additional information through grand jury subpoenas that could help to uncover more substantial monetary losses to the victims.

RECOMMENDATION: INCREASE PROSECUTIONS OF IDENTITY THEFT

The Task Force recommends that, to further increase the number of prosecutions of identity thieves, the following steps should be taken:

- **Designate An Identity Theft Coordinator for Each United States Attorney's Office To Design a Specific Identity Theft Program for Each District.** DOJ should direct that each U.S. Attorney's Office, by June 2007, designate one Assistant U.S. Attorney who should serve as a point of contact and source of expertise within that office for other prosecutors and agents. That Assistant U.S. Attorney also should assist each U.S. Attorney in making a district-specific determination about the areas on which to focus to best address the problem of identity theft. For example, in some southwest border districts, identity theft may be best addressed by stepping up efforts to prosecute immigration fraud. In other districts, identity theft may be best addressed by increasing prosecutions of bank fraud schemes or by making an effort to add identity theft violations to the charges that are brought against those who commit wire/mail/bank fraud schemes through the misappropriation of identities.
- **Evaluate Monetary Thresholds for Prosecution.** By June 2007, the investigative agencies and U.S. Attorney's Offices should re-evaluate current monetary thresholds for initiating identity theft cases and, specifically, should consider whether monetary thresholds for accepting such cases for prosecution should be lowered in light of the fact that investigations often reveal additional loss and additional victims, that monetary loss may not always adequately reflect the harm suffered, and that the aggravated identity theft statute makes it possible for the government to obtain significant sentences even in cases where precisely calculating the monetary loss is difficult or impossible.
- **Encourage State Prosecution of Identity Theft.** DOJ should explore ways to increase resources and training for local investigators and prosecutors handling identity theft cases. Moreover, each U.S. Attorney, by June 2007, should engage in discussions with state and local prosecutors in his or her district to encourage those prosecutors to accept cases that do not meet appropriately-set thresholds for federal prosecution, with the understanding that these cases need not always be brought as identity theft cases.

- **Create Working Groups and Task Forces.** By the end of 2007, U.S. Attorneys and investigative agencies should create or make increased use of interagency working groups and task forces devoted to identity theft. Where funds for a task force are unavailable, consideration should be given to forming working groups with non-dedicated personnel.

RECOMMENDATION: CONDUCT TARGETED ENFORCEMENT INITIATIVES

Law enforcement agencies should continue to conduct enforcement initiatives that focus exclusively or primarily on identity theft. The initiatives should pursue the following:

- **Unfair or Deceptive Means to Make SSNs Available for Sale.** Beginning immediately, law enforcement should more aggressively target the community of businesses on the Internet that sell individuals' SSNs or other sensitive information to anyone who provides them with the individual's name and other limited information. The SSA OIG and other agencies also should continue or initiate investigations of entities that use unlawful means to make SSNs and other sensitive personal information available for sale.

- **Identity Theft Related to the Health Care System.** HHS should continue to investigate identity theft related to Medicare fraud. As part of this effort, HHS should begin to work with state authorities immediately to provide for stronger state licensure and certification of providers, practitioners, and suppliers. Schemes to defraud Medicare may involve the theft of beneficiaries' and providers' identities and identification numbers, the opening of bank accounts in individuals' names, and the submission of fraudulent Medicare claims. Medicare payment is linked to state licensure and certification of providers, practitioners, and suppliers as business entities. Lack of state licensure and certification laws and/or laws that do not require identification and location information of owners and officers of providers, practitioners and suppliers, can hamper the ability of HHS to stop identity theft related to fraudulent billing of the Medicare program.

- **Identity Theft By Illegal Aliens.** Law enforcement agencies, particularly the Department of Homeland Security, should conduct targeted enforcement initiatives directed at illegal aliens who use stolen identities to enter or stay in the United States.

RECOMMENDATION: REVIEW CIVIL MONETARY PENALTY PROGRAMS

By the fourth quarter of 2007, federal agencies, including the SEC, the federal bank regulatory agencies, and the Department of Treasury, should review their civil monetary penalty programs to assess whether they adequately address identity theft. If they do not, analysis should be done as to what, if any, remedies, including legislation, would be appropriate, and any such legislation should be proposed by the first quarter of 2008. If a federal agency does not have a civil monetary penalty program, the establishment of such a program with respect to identity theft should be considered.

4. STATUTES CRIMINALIZING IDENTITY-THEFT RELATED OFFENSES: THE GAPS

Federal law enforcement has successfully investigated and prosecuted identity theft under a variety of criminal statutes. Effective prosecution can be hindered in some cases, however, as a result of certain gaps in those statutes. At the same time, a gap in one aspect of the U.S. Sentencing Guidelines has precluded some courts from enhancing the sentences for some identity thieves whose conduct affected multiple victims. See Volume II, Part N, for an additional description of federal criminal statutes used to prosecute identity theft.

a. The Identity Theft Statutes

The two federal statutes that directly criminalize identity theft are the identity theft statute (18 U.S.C. § 1028(a)(7)) and the aggravated identity theft statute (18 U.S.C. § 1028A(a)). The identity theft statute generally prohibits the possession or use of a means of identification of a person in connection with any unlawful activity that either constitutes a violation of federal law or that constitutes a felony under state or local law.[76] Similarly, the aggravated identity theft statute generally prohibits the possession or use of a means of identification of another person during the commission of, or in relation to, any of several enumerated federal felonies, and provides for enhanced penalties in those situations.

There are two gaps in these statutes, however. First, because both statutes are limited to the illegal use of a means of identification of "a person," it is unclear whether the government can prosecute an identity thief who misuses the means of identification of a corporation or organization, such as the name, logo, trademark, or employer identification number of a legitimate business. This gap means that federal prosecutors cannot use those statutes to charge identity thieves who, for example, create and use counterfeit documents or checks in the name of a corporation, or who engage in phishing schemes that use an organization's name. Second, the enumerated felonies in the aggravated identity theft statute do not include certain crimes that recur in identity theft and fraud cases, such as mail theft, uttering counterfeit securities, tax fraud, and conspiracy to commit certain offenses.

b. Computer-Related Identity Theft Statutes

Two of the federal statutes that apply to computer-related identity theft have similar limitations that preclude their use in certain important circumstances. First, 18 U.S.C. § 1030(a)(2) criminalizes the theft of information from a computer. However, federal courts only have jurisdiction if the thief uses an interstate communication to access the computer (unless the computer belongs to the federal government or a financial institution). As a result, the theft of personal information either by a corporate insider using the company's internal local networks, or by a thief intruding into a wireless network, generally would not involve an interstate communication and could not be prosecuted under this statute. In one case in North Carolina, for instance, an individual broke into a hospital computer's wireless network and thereby obtained patient information. State investigators and the victim asked the United States Attorney's Office to support the investigation and charge the criminal. Because the communications occurred wholly intrastate, however, no federal law criminalized the conduct.

A second limitation is found in 18 U.S.C. § 1030(a)(5), which criminalizes actions that cause "damage" to computers, i.e., that impair the "integrity or availability" of data or computer systems.[77] Absent special circumstances, the loss caused by the criminal conduct must exceed $5,000 to constitute a federal crime. Many identity thieves obtain personal information by installing malicious spyware, such as keyloggers, on many individuals' computers. Whether the programs succeed in obtaining the unsuspecting computer owner's financial data, these sorts of programs harm the "integrity" of the computer and data. Nevertheless, it is often difficult or impossible to measure the loss this damage causes to each computer owner, or to prove that the total value of these many small losses exceeds $5,000.

c. Cyber-Extortion Statute

Another federal criminal statute that may apply in some computer-related identity theft cases is the "cyber-extortion" provision of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(7). This provision, which prohibits the transmission of a threat "to cause damage to a protected computer,"[78] is used to prosecute criminals who threaten to delete data, crash computers, or knock computers off of the Internet using a denial of service attack. Some cyber-criminals extort companies, however, without explicitly threatening to cause damage to computers. Instead, they steal confidential data and then threaten to make it public if their demands are not met. In other cases, the criminal causes the damage first—such as by accessing a corporate computer without authority and encrypting critical data—and then threatens not to correct the problem unless the victim pays. Thus, the requirement in section 1030(a)(7) that the defendant must explicitly "threaten to cause damage" can preclude successful prosecutions for cyber-extortion under this statute under certain circumstances.

d. Sentencing Guidelines Governing Identity Theft

In recent years, the courts have created some uncertainty about the applicability of the "multiple victim enhancement" provision of the U.S. Sentencing Guidelines in identity theft cases. This provision allows courts to increase the sentence for an identity thief who victimizes more than one person. It is unclear, however, whether this sentencing enhancement applies when the victims have not sustained actual monetary loss. For example, in some jurisdictions, when a financial institution indemnifies 20 victims of unauthorized charges to their credit cards, the courts consider the financial institution to be the only victim. In such cases, the identity thief therefore may not be penalized for having engaged in conduct that harmed 20 people, simply because those 20 people were later indemnified. This interpretation of the Sentencing Guidelines conflicts with a primary purpose of the Identity Theft and Assumption Deterrence Act of 1998: to vindicate the interests of individual identity theft victims.[79]

▶ RECOMMENDATION: CLOSE THE GAPS IN FEDERAL CRIMINAL STATUTES USED TO PROSECUTE IDENTITY-THEFT RELATED OFFENSES TO ENSURE INCREASED FEDERAL PROSECUTION OF THESE CRIMES

The Task Force recommends that Congress take the following legislative actions:

▶ **Amend the Identity Theft and Aggravated Identity Theft Statutes to Ensure That Identity Thieves Who Misappropriate Information Belonging to Corporations and Organizations Can Be Prosecuted.** Proposed amendments to 18 U.S.C. §§ 1028 and 1028A are available in Appendix E.

- **Add Several New Crimes to the List of Predicate Offenses for Aggravated Identity Theft Offenses.** The aggravated identity theft statute, 18 U.S.C. § 1028A, should include other federal offenses that recur in various identity-theft and fraud cases—mail theft, uttering counterfeit securities, and tax fraud, as well as conspiracy to commit specified felonies already listed in 18 U.S.C. § 1028A—in the statutory list of predicate offenses for that offense. Proposed additions to 18 U.S.C. § 1028A are contained in Appendix E.
- **Amend the Statute That Criminalizes the Theft of Electronic Data By Eliminating the Current Requirement That the Information Must Have Been Stolen Through Interstate Communications.** The proposed amendment to 18 U.S.C. § 1030(a)(2) is available in Appendix F.
- **Penalize Malicious Spyware and Keyloggers.** The statutory provisions in 18 U.S.C. § 1030(a)(5) should be amended to penalize appropriately the use of malicious spyware and keyloggers, by eliminating the current requirement that the defendant's action must cause "damage" to computers and that the loss caused by the conduct must exceed $5,000. Proposed amendments to 18 U.S.C. §§ 1030(a)(5), (c), and (g), and the accompanying amendment to 18 U.S.C. § 2332b(g), are included in Appendix G.
- **Amend the Cyber-Extortion Statute to Cover Additional, Alternate Types of Cyber-Extortion.** The proposed amendment to 18 U.S.C. § 1030(a)(7) is available in Appendix H.

RECOMMENDATION: ENSURE THAT AN IDENTITY THIEF'S SENTENCE CAN BE ENHANCED WHEN THE CRIMINAL CONDUCT AFFECTS MORE THAN ONE VICTIM

The Sentencing Commission should amend the definition of "victim," as that term is used under United States Sentencing Guideline section 2B1.1, to state clearly that a victim need not have sustained an actual monetary loss. This amendment will ensure that courts can enhance the sentences imposed on identity thieves who cause harm to multiple victims, even when that harm does not result in any monetary loss to the victims. The proposed amendment to United States Sentencing Guideline section 2B1.1 is available in Appendix I.

5. *TRAINING OF LAW ENFORCEMENT OFFICERS AND PROSECUTORS*

Training can be the key to effective investigations and prosecutions, and much has been done in recent years to ensure that investigators and prosecutors have been trained on topics relating to identity theft. In addition to ongoing training by U.S. Attorney's Offices, for example, several federal law enforcement agencies—including DOJ, the Postal Inspection Service, the Secret Service, the FTC, and the FBI—along with the American Association of Motor Vehicle Administrators (AAMVA) have sponsored jointly over 20 regional, one-day training seminars on identity fraud for state and local law enforcement agencies across the country. See Volume II, Part O, for a description of training by and for investigators and prosecutors.

Nonetheless, the amount, focus, and coordination of law enforcement training should be expanded. Identity theft investigations and prosecutions involve particular challenges—including the need to coordinate with foreign authorities, some difficulties with the application of the Sentencing Guidelines, and the challenges that arise from the inevitable gap in time between the commission of the identity theft and the reporting of the identity theft—that warrant more specialized training at all levels of law enforcement.

RECOMMENDATION: ENHANCE TRAINING FOR LAW ENFORCEMENT OFFICERS AND PROSECUTORS

- **Develop Course at National Advocacy Center (NAC) Focused Solely on Investigation and Prosecution of Identity Theft**. By the third quarter of 2007, DOJ's Office of Legal Education should complete the development of a course specifically focused on identity theft for prosecutors. The identity theft course should include, among other things: a review of the scope of the problem; a review of applicable statutes, forfeiture and sentencing guideline applications; an outline of investigative and case presentation techniques; training on addressing the unique needs of identity theft victims; and a review of programs for better utilizing collective resources (working groups, task forces, and any "model programs"— fast track programs, etc.).
- **Increase Number of Regional Identity Theft Seminars.** In 2006, the federal agencies and the AAMVA held a number of regional identity theft seminars for state and local law enforcement officers. In 2007, the number of seminars should be increased. Additionally, the participating entities should coordinate with the Task Force to provide the most complete, targeted, and up-to-date training materials.

- **Increase Resources for Law Enforcement Available on the Internet.** The identity theft clearinghouse site, ***www.idtheft.gov***, should be used as the portal for law enforcement agencies to gain access to additional educational materials on investigating identity theft and responding to victims.

- **Review Curricula to Enhance Basic and Advanced Training on Identity Theft.** By the fourth quarter of 2007, federal investigative agencies should review their own training curricula, and curricula of the Federal Law Enforcement Training Center, to ensure that they are providing the most useful training on identity theft.

6. MEASURING SUCCESS OF LAW ENFORCEMENT EFFORTS

One shortcoming in the federal government's ability to understand and respond effectively to identity theft is the lack of comprehensive statistical data about the success of law enforcement efforts to combat identity theft. Specifically, there are few benchmarks that measure the activities of the various components of the criminal justice system in their response to identity thefts occurring within their jurisdictions, little data on state and local enforcement, and little information on how identity theft incidents are being processed in state courts.

Addressing these questions requires benchmarks and periodic data collection. The Bureau of Justice Statistics (BJS) has platforms in place, as well as the tools to create new platforms, to obtain information about identity theft from victims and the response to identity theft from law enforcement agencies, state and federal prosecutors, and courts.

RECOMMENDATION: ENHANCE THE GATHERING OF STATISTICAL DATA MEASURING THE CRIMINAL JUSTICE SYSTEM'S RESPONSE TO IDENTITY THEFT

- **Gather and Analyze Statistically Reliable Data from Identity Theft Victims.** The BJS and FTC should continue to gather and analyze statistically reliable data from identity theft victims. The BJS should conduct its surveys in collaboration with subject matter experts from the FTC. BJS should add additional questions on identity theft to the household portion of its National Crime Victimization Survey (NCVS), and conduct periodic supplements to gather more in-depth information. The FTC should conduct a general identity theft survey approximately every three years, independently or in conjunction with BJS or other government agencies. The FTC also should conduct surveys focused more narrowly on issues related to the effectiveness of and compliance with the identity theft-related provisions of the consumer protection laws it enforces.

- **Expand Scope of National Crime Victimization Survey (NCVS).** The scope of the annual NCVS should be expanded to collect information about the characteristics, consequences, and extent of identity theft for individuals ages 12 and older. Currently, information on identity theft is collected only from the household respondent and does not capture data on multiple victims in the household or multiple episodes of identity theft.

- **Review of Sentencing Commission Data.** DOJ and the FTC should systematically review and analyze U.S. Sentencing Commission identity theft-related case files every two to four years, and should begin in the third quarter of 2007.

- **Track Prosecutions of Identity Theft and the Amount of Resources Spent.** In order to better track resources spent on identity theft cases, DOJ should, by the second quarter of 2007, create an "Identity Theft" category on the monthly report that is completed by all Assistant United States Attorneys, and should revise its departmental case tracking application to allow for the reporting of offenses by individual subsections of section 1028. Additionally, BJS should incorporate additional questions in the National Survey of Prosecutors to better understand the impact identity theft is having on prosecutorial resources.

- **Conduct Targeted Surveys.** In order to expand law enforcement knowledge of the identity theft response and prevention activities of state and local police, BJS should undertake new data collections in specified areas. Proposed details of those surveys are included in Appendix J.

IV. Conclusion: The Way Forward

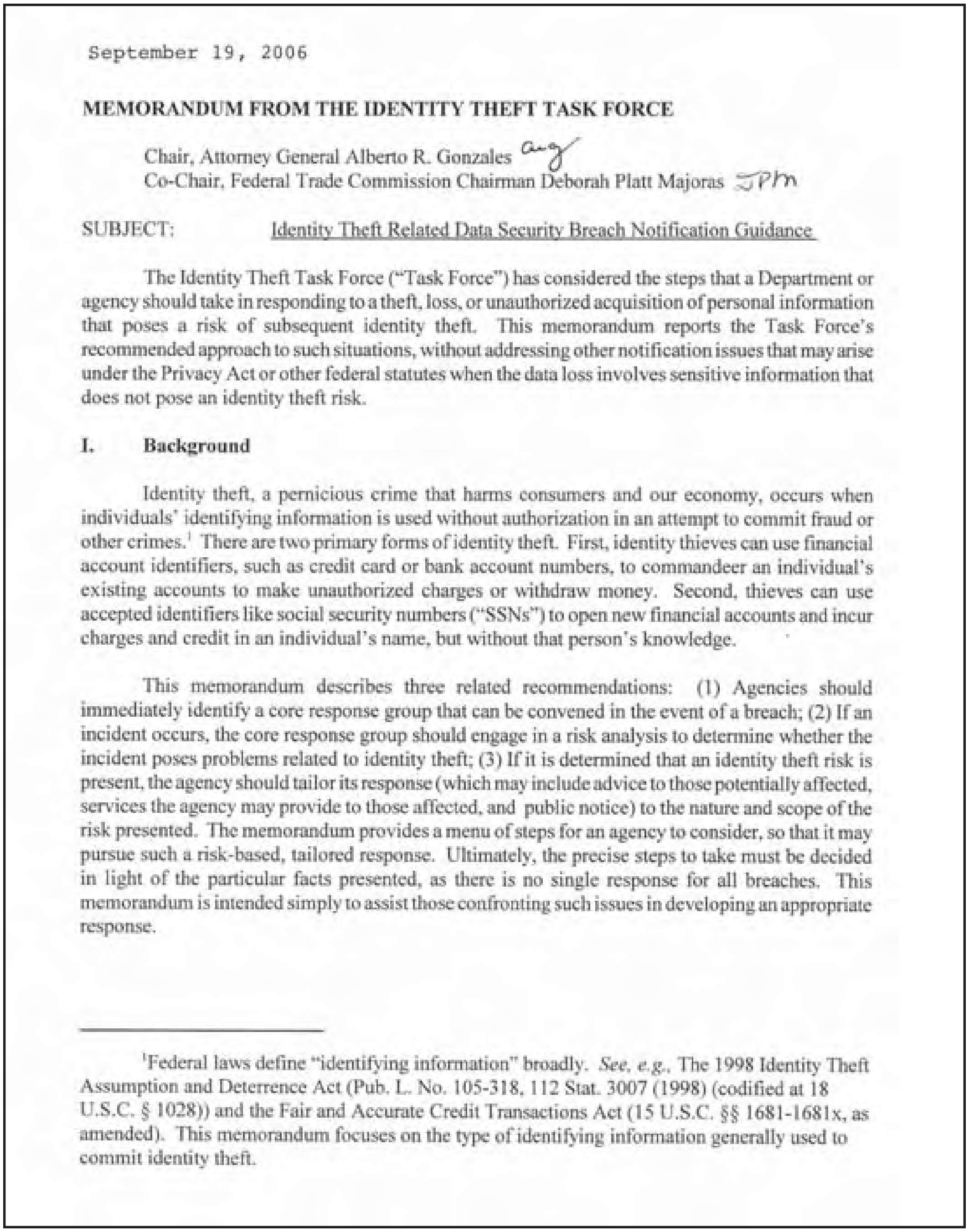
There is no magic bullet that will eradicate identity theft. To successfully combat identity theft and its effects, we must keep personal information out of the hands of thieves; take steps to prevent an identity thief from misusing any data that may end up in his hands; prosecute him vigorously if he succeeds in committing the crime; and do all we can to help the victims recover.

Only a comprehensive and fully coordinated strategy to combat identity theft—one that encompasses effective prevention, public awareness and education, victim assistance, and law enforcement measures, and that fully engages federal, state, and local authorities and the private sector—will have any chance of solving the problem. This proposed strategic plan strives to set out such a comprehensive approach to combating identity theft, but it is only the beginning. Each of the stakeholders—consumers, business and government—must fully and actively participate in this fight for us to succeed, and must stay attuned to emerging trends in order to adapt and respond to developing threats to consumer well being.

Appendices

APPENDIX A

Identity Theft Task Force's Guidance Memorandum on Data Breach Protocol



September 19, 2006

MEMORANDUM FROM THE IDENTITY THEFT TASK FORCE

Chair, Attorney General Alberto R. Gonzales arg
Co-Chair, Federal Trade Commission Chairman Deborah Platt Majoras DPM

SUBJECT: Identity Theft Related Data Security Breach Notification Guidance

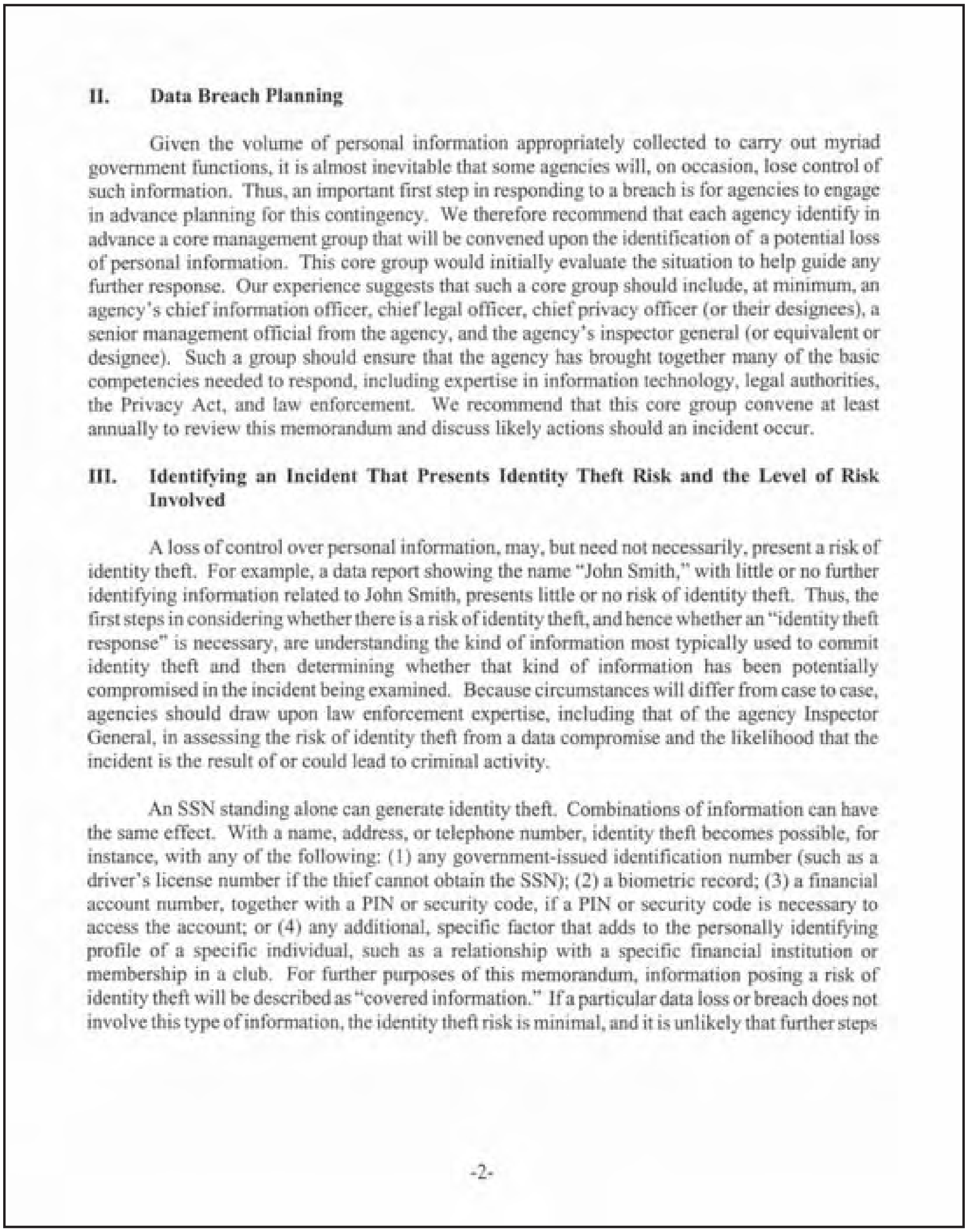
The Identity Theft Task Force ("Task Force") has considered the steps that a Department or agency should take in responding to a theft, loss, or unauthorized acquisition of personal information that poses a risk of subsequent identity theft. This memorandum reports the Task Force's recommended approach to such situations, without addressing other notification issues that may arise under the Privacy Act or other federal statutes when the data loss involves sensitive information that does not pose an identity theft risk.

I. Background

Identity theft, a pernicious crime that harms consumers and our economy, occurs when individuals' identifying information is used without authorization in an attempt to commit fraud or other crimes.[1] There are two primary forms of identity theft. First, identity thieves can use financial account identifiers, such as credit card or bank account numbers, to commandeer an individual's existing accounts to make unauthorized charges or withdraw money. Second, thieves can use accepted identifiers like social security numbers ("SSNs") to open new financial accounts and incur charges and credit in an individual's name, but without that person's knowledge.

This memorandum describes three related recommendations: (1) Agencies should immediately identify a core response group that can be convened in the event of a breach; (2) If an incident occurs, the core response group should engage in a risk analysis to determine whether the incident poses problems related to identity theft; (3) If it is determined that an identity theft risk is present, the agency should tailor its response (which may include advice to those potentially affected, services the agency may provide to those affected, and public notice) to the nature and scope of the risk presented. The memorandum provides a menu of steps for an agency to consider, so that it may pursue such a risk-based, tailored response. Ultimately, the precise steps to take must be decided in light of the particular facts presented, as there is no single response for all breaches. This memorandum is intended simply to assist those confronting such issues in developing an appropriate response.

[1] Federal laws define "identifying information" broadly. *See, e.g.*, The 1998 Identity Theft Assumption and Deterrence Act (Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028)) and the Fair and Accurate Credit Transactions Act (15 U.S.C. §§ 1681-1681x, as amended). This memorandum focuses on the type of identifying information generally used to commit identity theft.



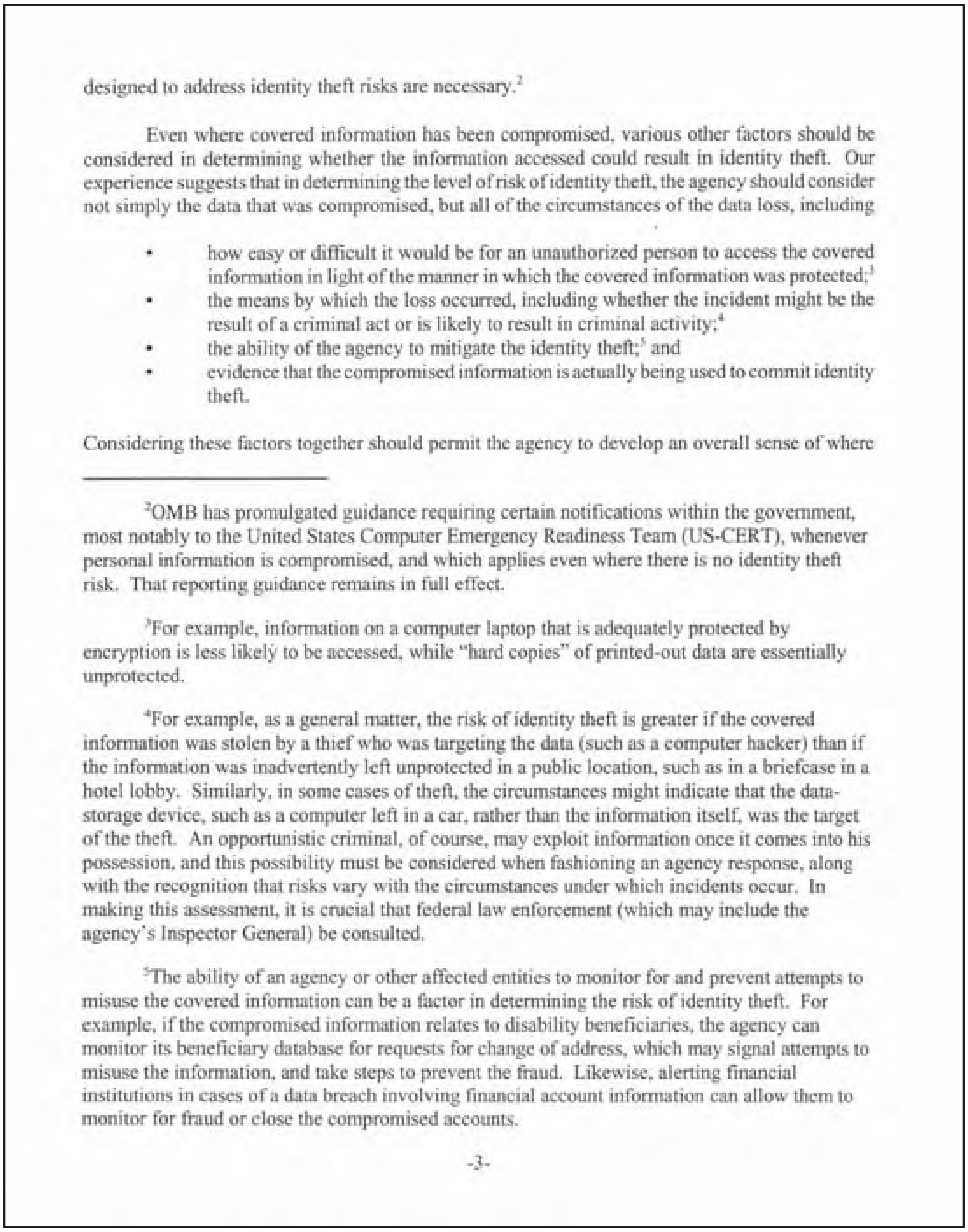
II. Data Breach Planning

Given the volume of personal information appropriately collected to carry out myriad government functions, it is almost inevitable that some agencies will, on occasion, lose control of such information. Thus, an important first step in responding to a breach is for agencies to engage in advance planning for this contingency. We therefore recommend that each agency identify in advance a core management group that will be convened upon the identification of a potential loss of personal information. This core group would initially evaluate the situation to help guide any further response. Our experience suggests that such a core group should include, at minimum, an agency's chief information officer, chief legal officer, chief privacy officer (or their designees), a senior management official from the agency, and the agency's inspector general (or equivalent or designee). Such a group should ensure that the agency has brought together many of the basic competencies needed to respond, including expertise in information technology, legal authorities, the Privacy Act, and law enforcement. We recommend that this core group convene at least annually to review this memorandum and discuss likely actions should an incident occur.

III. Identifying an Incident That Presents Identity Theft Risk and the Level of Risk Involved

A loss of control over personal information, may, but need not necessarily, present a risk of identity theft. For example, a data report showing the name "John Smith," with little or no further identifying information related to John Smith, presents little or no risk of identity theft. Thus, the first steps in considering whether there is a risk of identity theft, and hence whether an "identity theft response" is necessary, are understanding the kind of information most typically used to commit identity theft and then determining whether that kind of information has been potentially compromised in the incident being examined. Because circumstances will differ from case to case, agencies should draw upon law enforcement expertise, including that of the agency Inspector General, in assessing the risk of identity theft from a data compromise and the likelihood that the incident is the result of or could lead to criminal activity.

An SSN standing alone can generate identity theft. Combinations of information can have the same effect. With a name, address, or telephone number, identity theft becomes possible, for instance, with any of the following: (1) any government-issued identification number (such as a driver's license number if the thief cannot obtain the SSN); (2) a biometric record; (3) a financial account number, together with a PIN or security code, if a PIN or security code is necessary to access the account; or (4) any additional, specific factor that adds to the personally identifying profile of a specific individual, such as a relationship with a specific financial institution or membership in a club. For further purposes of this memorandum, information posing a risk of identity theft will be described as "covered information." If a particular data loss or breach does not involve this type of information, the identity theft risk is minimal, and it is unlikely that further steps



designed to address identity theft risks are necessary.[2]

Even where covered information has been compromised, various other factors should be considered in determining whether the information accessed could result in identity theft. Our experience suggests that in determining the level of risk of identity theft, the agency should consider not simply the data that was compromised, but all of the circumstances of the data loss, including

- how easy or difficult it would be for an unauthorized person to access the covered information in light of the manner in which the covered information was protected;[3]
- the means by which the loss occurred, including whether the incident might be the result of a criminal act or is likely to result in criminal activity;[4]
- the ability of the agency to mitigate the identity theft;[5] and
- evidence that the compromised information is actually being used to commit identity theft.

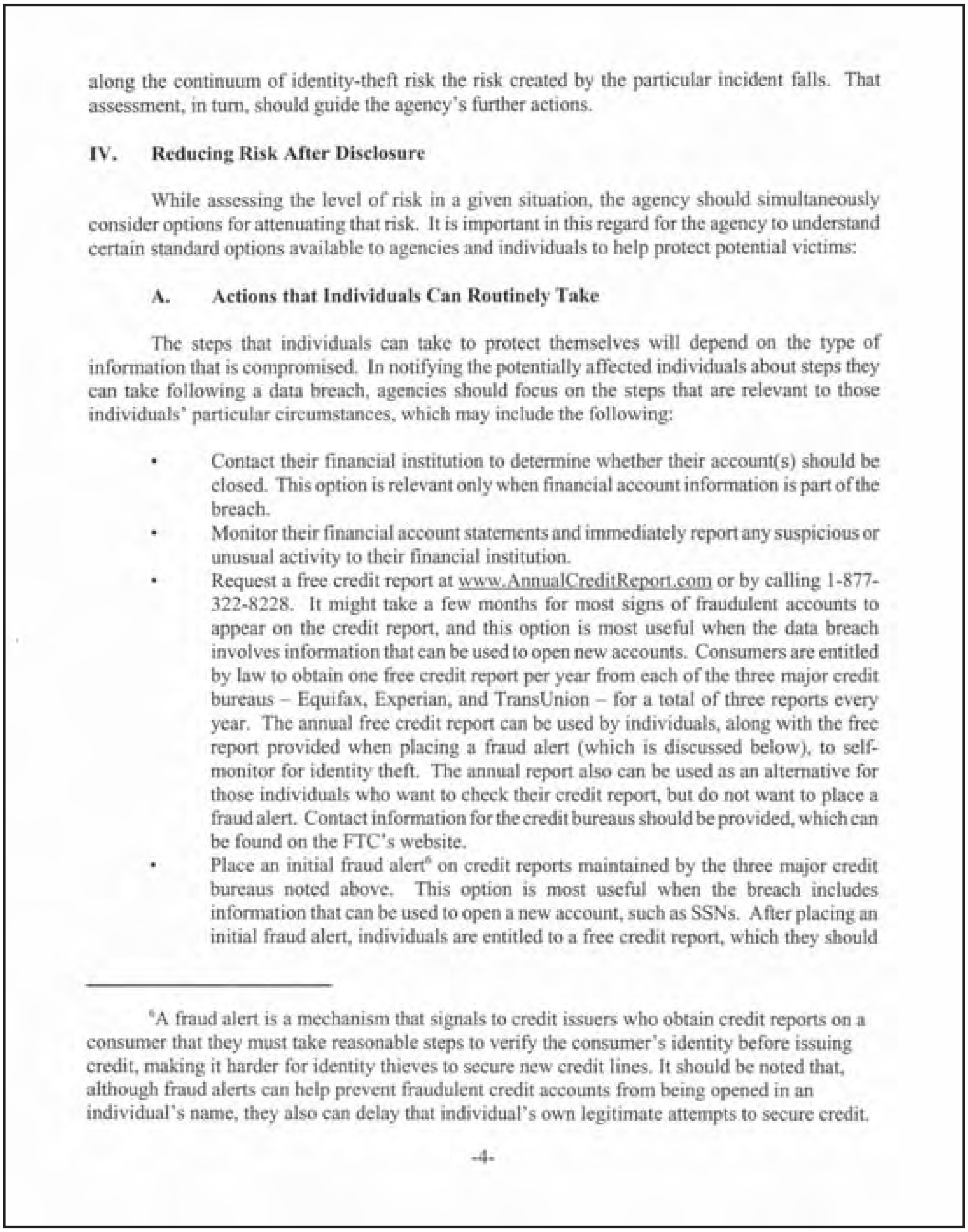
Considering these factors together should permit the agency to develop an overall sense of where

[2] OMB has promulgated guidance requiring certain notifications within the government, most notably to the United States Computer Emergency Readiness Team (US-CERT), whenever personal information is compromised, and which applies even where there is no identity theft risk. That reporting guidance remains in full effect.

[3] For example, information on a computer laptop that is adequately protected by encryption is less likely to be accessed, while "hard copies" of printed-out data are essentially unprotected.

[4] For example, as a general matter, the risk of identity theft is greater if the covered information was stolen by a thief who was targeting the data (such as a computer hacker) than if the information was inadvertently left unprotected in a public location, such as in a briefcase in a hotel lobby. Similarly, in some cases of theft, the circumstances might indicate that the data-storage device, such as a computer left in a car, rather than the information itself, was the target of the theft. An opportunistic criminal, of course, may exploit information once it comes into his possession, and this possibility must be considered when fashioning an agency response, along with the recognition that risks vary with the circumstances under which incidents occur. In making this assessment, it is crucial that federal law enforcement (which may include the agency's Inspector General) be consulted.

[5] The ability of an agency or other affected entities to monitor for and prevent attempts to misuse the covered information can be a factor in determining the risk of identity theft. For example, if the compromised information relates to disability beneficiaries, the agency can monitor its beneficiary database for requests for change of address, which may signal attempts to misuse the information, and take steps to prevent the fraud. Likewise, alerting financial institutions in cases of a data breach involving financial account information can allow them to monitor for fraud or close the compromised accounts.



along the continuum of identity-theft risk the risk created by the particular incident falls. That assessment, in turn, should guide the agency's further actions.

IV. Reducing Risk After Disclosure

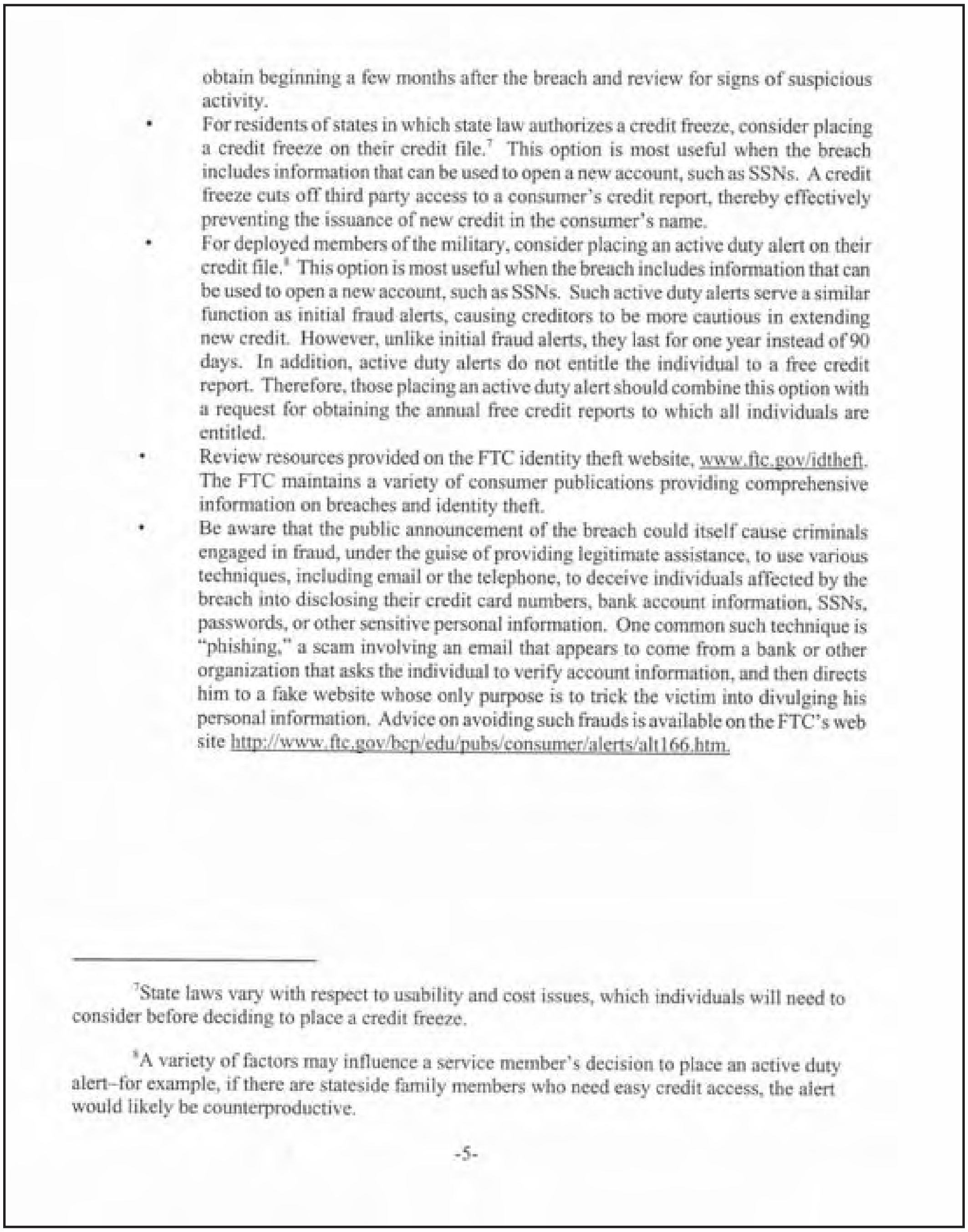
While assessing the level of risk in a given situation, the agency should simultaneously consider options for attenuating that risk. It is important in this regard for the agency to understand certain standard options available to agencies and individuals to help protect potential victims:

A. Actions that Individuals Can Routinely Take

The steps that individuals can take to protect themselves will depend on the type of information that is compromised. In notifying the potentially affected individuals about steps they can take following a data breach, agencies should focus on the steps that are relevant to those individuals' particular circumstances, which may include the following:

- Contact their financial institution to determine whether their account(s) should be closed. This option is relevant only when financial account information is part of the breach.
- Monitor their financial account statements and immediately report any suspicious or unusual activity to their financial institution.
- Request a free credit report at www.AnnualCreditReport.com or by calling 1-877-322-8228. It might take a few months for most signs of fraudulent accounts to appear on the credit report, and this option is most useful when the data breach involves information that can be used to open new accounts. Consumers are entitled by law to obtain one free credit report per year from each of the three major credit bureaus – Equifax, Experian, and TransUnion – for a total of three reports every year. The annual free credit report can be used by individuals, along with the free report provided when placing a fraud alert (which is discussed below), to self-monitor for identity theft. The annual report also can be used as an alternative for those individuals who want to check their credit report, but do not want to place a fraud alert. Contact information for the credit bureaus should be provided, which can be found on the FTC's website.
- Place an initial fraud alert[6] on credit reports maintained by the three major credit bureaus noted above. This option is most useful when the breach includes information that can be used to open a new account, such as SSNs. After placing an initial fraud alert, individuals are entitled to a free credit report, which they should

[6] A fraud alert is a mechanism that signals to credit issuers who obtain credit reports on a consumer that they must take reasonable steps to verify the consumer's identity before issuing credit, making it harder for identity thieves to secure new credit lines. It should be noted that, although fraud alerts can help prevent fraudulent credit accounts from being opened in an individual's name, they also can delay that individual's own legitimate attempts to secure credit.

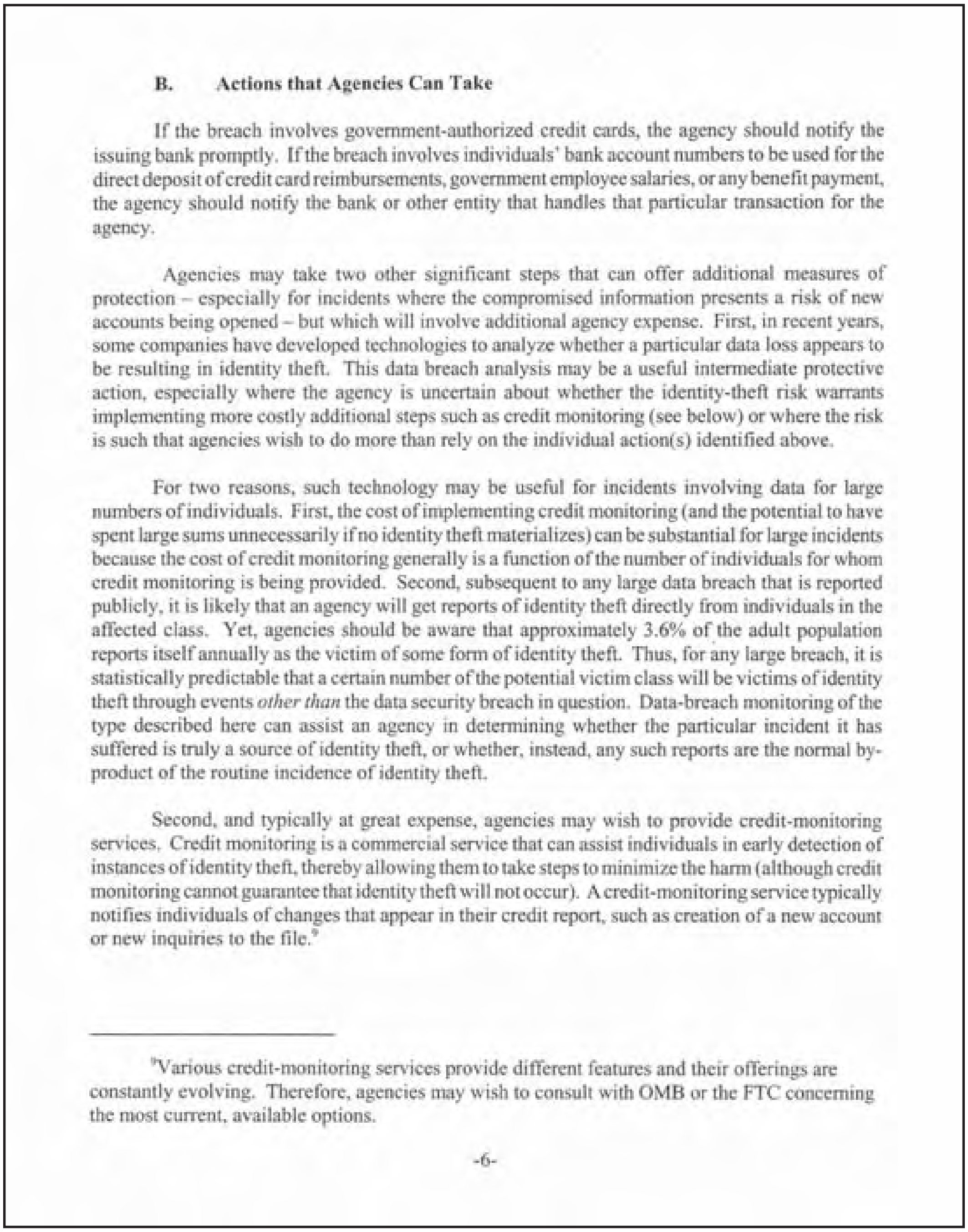


obtain beginning a few months after the breach and review for signs of suspicious activity.

- For residents of states in which state law authorizes a credit freeze, consider placing a credit freeze on their credit file.[7] This option is most useful when the breach includes information that can be used to open a new account, such as SSNs. A credit freeze cuts off third party access to a consumer's credit report, thereby effectively preventing the issuance of new credit in the consumer's name.
- For deployed members of the military, consider placing an active duty alert on their credit file.[8] This option is most useful when the breach includes information that can be used to open a new account, such as SSNs. Such active duty alerts serve a similar function as initial fraud alerts, causing creditors to be more cautious in extending new credit. However, unlike initial fraud alerts, they last for one year instead of 90 days. In addition, active duty alerts do not entitle the individual to a free credit report. Therefore, those placing an active duty alert should combine this option with a request for obtaining the annual free credit reports to which all individuals are entitled.
- Review resources provided on the FTC identity theft website, www.ftc.gov/idtheft. The FTC maintains a variety of consumer publications providing comprehensive information on breaches and identity theft.
- Be aware that the public announcement of the breach could itself cause criminals engaged in fraud, under the guise of providing legitimate assistance, to use various techniques, including email or the telephone, to deceive individuals affected by the breach into disclosing their credit card numbers, bank account information, SSNs, passwords, or other sensitive personal information. One common such technique is "phishing," a scam involving an email that appears to come from a bank or other organization that asks the individual to verify account information, and then directs him to a fake website whose only purpose is to trick the victim into divulging his personal information. Advice on avoiding such frauds is available on the FTC's web site http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt166.htm.

[7] State laws vary with respect to usability and cost issues, which individuals will need to consider before deciding to place a credit freeze.

[8] A variety of factors may influence a service member's decision to place an active duty alert–for example, if there are stateside family members who need easy credit access, the alert would likely be counterproductive.



B. Actions that Agencies Can Take

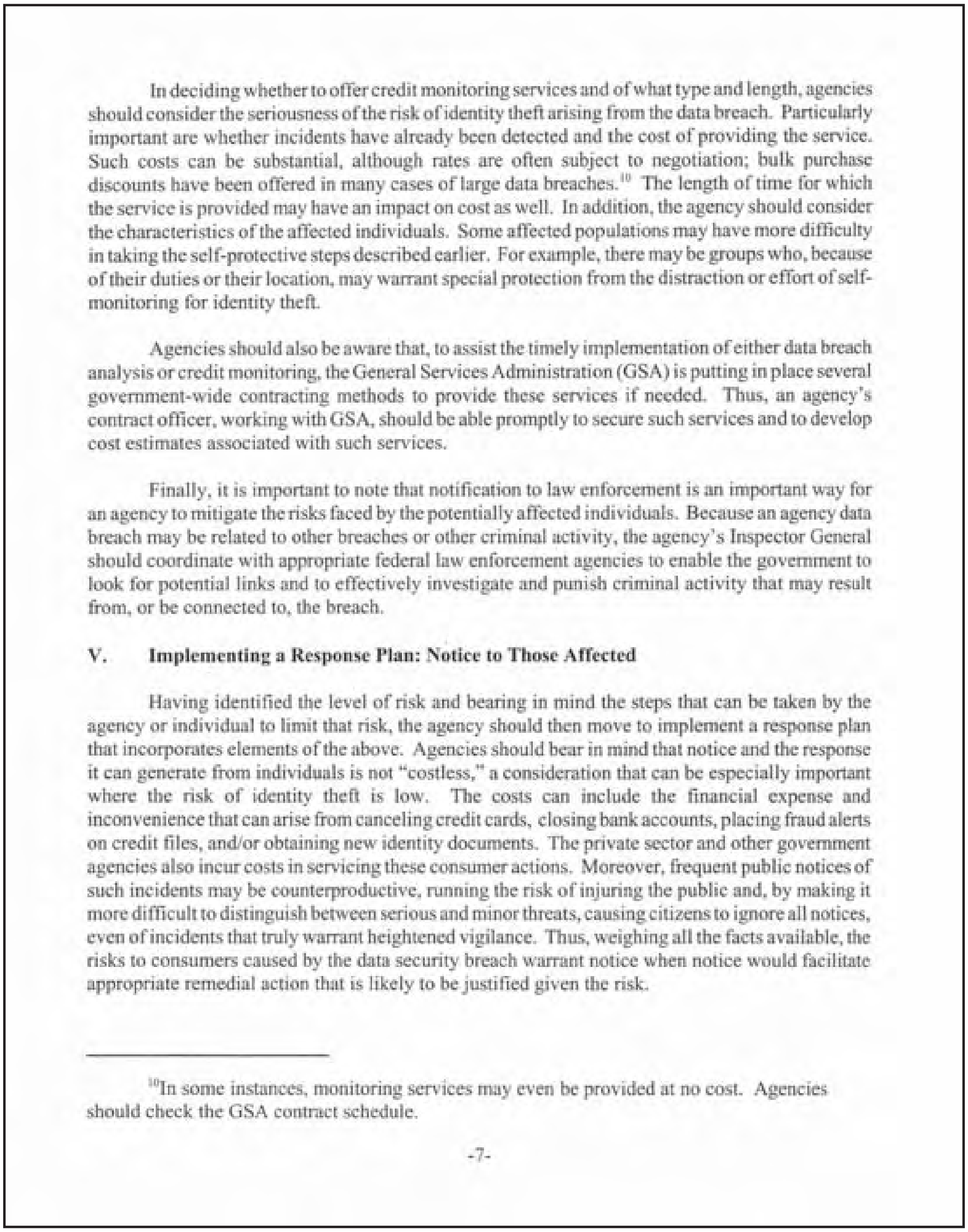
If the breach involves government-authorized credit cards, the agency should notify the issuing bank promptly. If the breach involves individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government employee salaries, or any benefit payment, the agency should notify the bank or other entity that handles that particular transaction for the agency.

Agencies may take two other significant steps that can offer additional measures of protection – especially for incidents where the compromised information presents a risk of new accounts being opened – but which will involve additional agency expense. First, in recent years, some companies have developed technologies to analyze whether a particular data loss appears to be resulting in identity theft. This data breach analysis may be a useful intermediate protective action, especially where the agency is uncertain about whether the identity-theft risk warrants implementing more costly additional steps such as credit monitoring (see below) or where the risk is such that agencies wish to do more than rely on the individual action(s) identified above.

For two reasons, such technology may be useful for incidents involving data for large numbers of individuals. First, the cost of implementing credit monitoring (and the potential to have spent large sums unnecessarily if no identity theft materializes) can be substantial for large incidents because the cost of credit monitoring generally is a function of the number of individuals for whom credit monitoring is being provided. Second, subsequent to any large data breach that is reported publicly, it is likely that an agency will get reports of identity theft directly from individuals in the affected class. Yet, agencies should be aware that approximately 3.6% of the adult population reports itself annually as the victim of some form of identity theft. Thus, for any large breach, it is statistically predictable that a certain number of the potential victim class will be victims of identity theft through events *other than* the data security breach in question. Data-breach monitoring of the type described here can assist an agency in determining whether the particular incident it has suffered is truly a source of identity theft, or whether, instead, any such reports are the normal by-product of the routine incidence of identity theft.

Second, and typically at great expense, agencies may wish to provide credit-monitoring services. Credit monitoring is a commercial service that can assist individuals in early detection of instances of identity theft, thereby allowing them to take steps to minimize the harm (although credit monitoring cannot guarantee that identity theft will not occur). A credit-monitoring service typically notifies individuals of changes that appear in their credit report, such as creation of a new account or new inquiries to the file.[9]

[9] Various credit-monitoring services provide different features and their offerings are constantly evolving. Therefore, agencies may wish to consult with OMB or the FTC concerning the most current, available options.



In deciding whether to offer credit monitoring services and of what type and length, agencies should consider the seriousness of the risk of identity theft arising from the data breach. Particularly important are whether incidents have already been detected and the cost of providing the service. Such costs can be substantial, although rates are often subject to negotiation; bulk purchase discounts have been offered in many cases of large data breaches.[10] The length of time for which the service is provided may have an impact on cost as well. In addition, the agency should consider the characteristics of the affected individuals. Some affected populations may have more difficulty in taking the self-protective steps described earlier. For example, there may be groups who, because of their duties or their location, may warrant special protection from the distraction or effort of self-monitoring for identity theft.

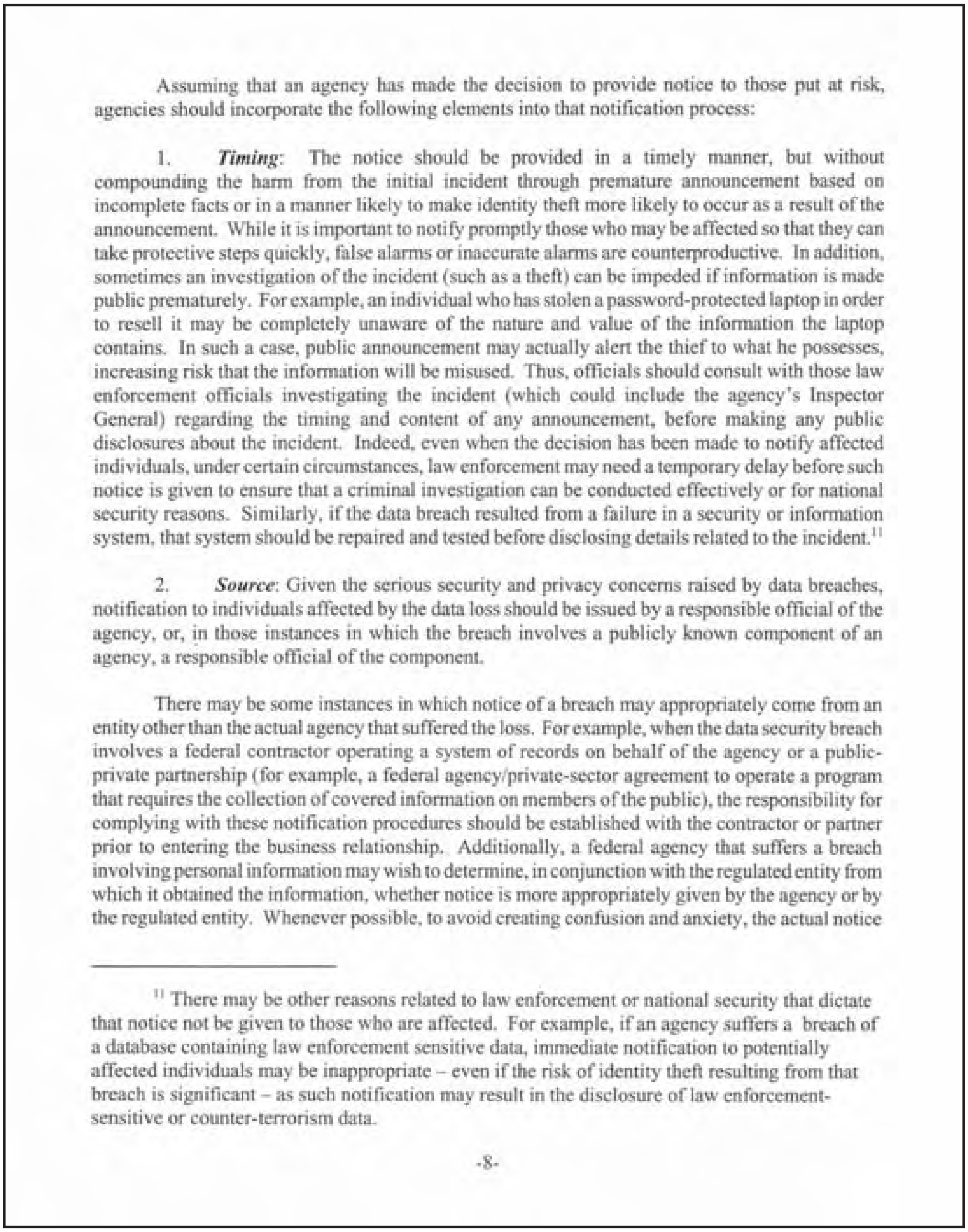
Agencies should also be aware that, to assist the timely implementation of either data breach analysis or credit monitoring, the General Services Administration (GSA) is putting in place several government-wide contracting methods to provide these services if needed. Thus, an agency's contract officer, working with GSA, should be able promptly to secure such services and to develop cost estimates associated with such services.

Finally, it is important to note that notification to law enforcement is an important way for an agency to mitigate the risks faced by the potentially affected individuals. Because an agency data breach may be related to other breaches or other criminal activity, the agency's Inspector General should coordinate with appropriate federal law enforcement agencies to enable the government to look for potential links and to effectively investigate and punish criminal activity that may result from, or be connected to, the breach.

V. Implementing a Response Plan: Notice to Those Affected

Having identified the level of risk and bearing in mind the steps that can be taken by the agency or individual to limit that risk, the agency should then move to implement a response plan that incorporates elements of the above. Agencies should bear in mind that notice and the response it can generate from individuals is not "costless," a consideration that can be especially important where the risk of identity theft is low. The costs can include the financial expense and inconvenience that can arise from canceling credit cards, closing bank accounts, placing fraud alerts on credit files, and/or obtaining new identity documents. The private sector and other government agencies also incur costs in servicing these consumer actions. Moreover, frequent public notices of such incidents may be counterproductive, running the risk of injuring the public and, by making it more difficult to distinguish between serious and minor threats, causing citizens to ignore all notices, even of incidents that truly warrant heightened vigilance. Thus, weighing all the facts available, the risks to consumers caused by the data security breach warrant notice when notice would facilitate appropriate remedial action that is likely to be justified given the risk.

[10] In some instances, monitoring services may even be provided at no cost. Agencies should check the GSA contract schedule.



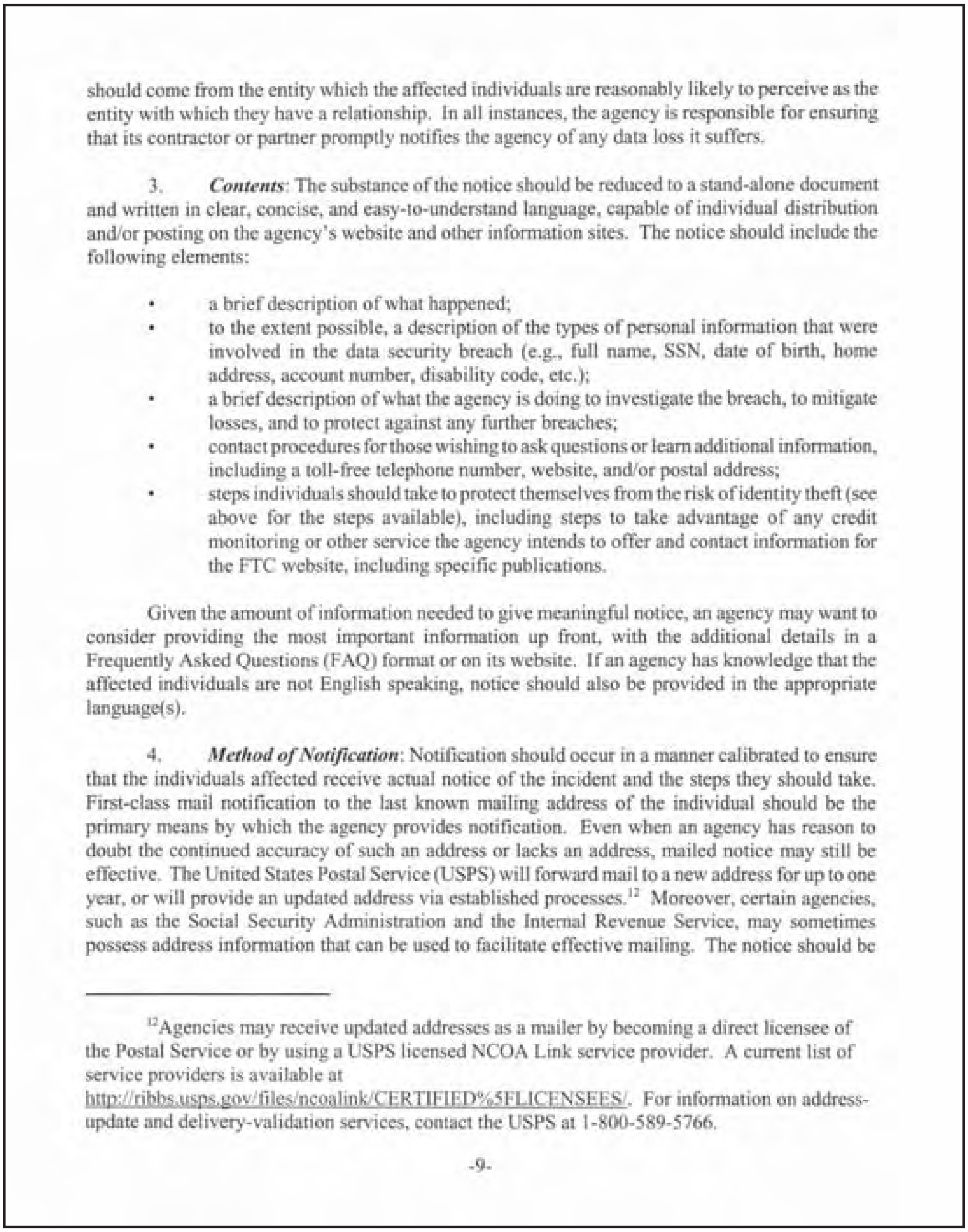
Assuming that an agency has made the decision to provide notice to those put at risk, agencies should incorporate the following elements into that notification process:

1. ***Timing***: The notice should be provided in a timely manner, but without compounding the harm from the initial incident through premature announcement based on incomplete facts or in a manner likely to make identity theft more likely to occur as a result of the announcement. While it is important to notify promptly those who may be affected so that they can take protective steps quickly, false alarms or inaccurate alarms are counterproductive. In addition, sometimes an investigation of the incident (such as a theft) can be impeded if information is made public prematurely. For example, an individual who has stolen a password-protected laptop in order to resell it may be completely unaware of the nature and value of the information the laptop contains. In such a case, public announcement may actually alert the thief to what he possesses, increasing risk that the information will be misused. Thus, officials should consult with those law enforcement officials investigating the incident (which could include the agency's Inspector General) regarding the timing and content of any announcement, before making any public disclosures about the incident. Indeed, even when the decision has been made to notify affected individuals, under certain circumstances, law enforcement may need a temporary delay before such notice is given to ensure that a criminal investigation can be conducted effectively or for national security reasons. Similarly, if the data breach resulted from a failure in a security or information system, that system should be repaired and tested before disclosing details related to the incident.[11]

2. ***Source***: Given the serious security and privacy concerns raised by data breaches, notification to individuals affected by the data loss should be issued by a responsible official of the agency, or, in those instances in which the breach involves a publicly known component of an agency, a responsible official of the component.

There may be some instances in which notice of a breach may appropriately come from an entity other than the actual agency that suffered the loss. For example, when the data security breach involves a federal contractor operating a system of records on behalf of the agency or a public-private partnership (for example, a federal agency/private-sector agreement to operate a program that requires the collection of covered information on members of the public), the responsibility for complying with these notification procedures should be established with the contractor or partner prior to entering the business relationship. Additionally, a federal agency that suffers a breach involving personal information may wish to determine, in conjunction with the regulated entity from which it obtained the information, whether notice is more appropriately given by the agency or by the regulated entity. Whenever possible, to avoid creating confusion and anxiety, the actual notice

[11] There may be other reasons related to law enforcement or national security that dictate that notice not be given to those who are affected. For example, if an agency suffers a breach of a database containing law enforcement sensitive data, immediate notification to potentially affected individuals may be inappropriate – even if the risk of identity theft resulting from that breach is significant – as such notification may result in the disclosure of law enforcement-sensitive or counter-terrorism data.



should come from the entity which the affected individuals are reasonably likely to perceive as the entity with which they have a relationship. In all instances, the agency is responsible for ensuring that its contractor or partner promptly notifies the agency of any data loss it suffers.

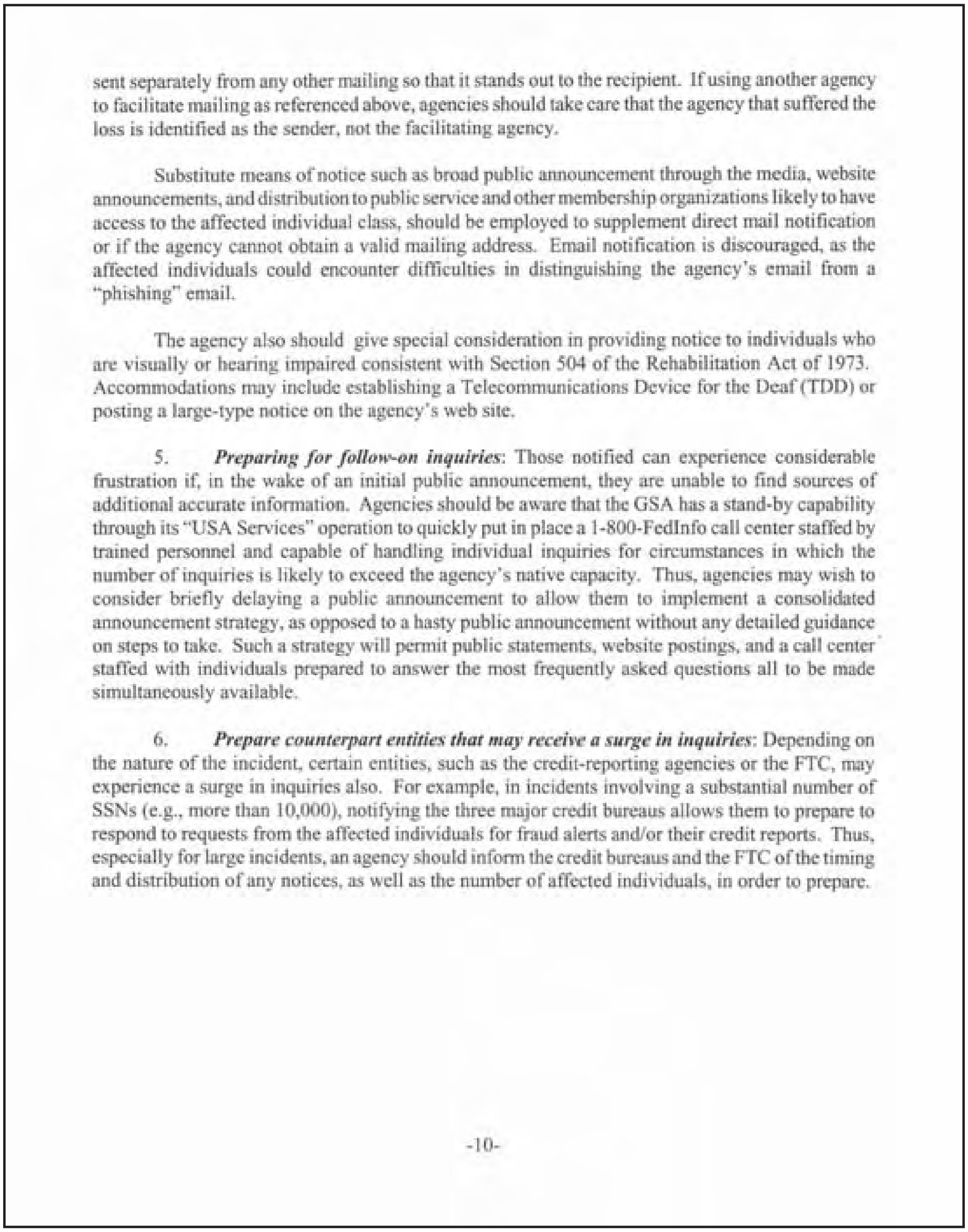
3. ***Contents***: The substance of the notice should be reduced to a stand-alone document and written in clear, concise, and easy-to-understand language, capable of individual distribution and/or posting on the agency's website and other information sites. The notice should include the following elements:

- a brief description of what happened;
- to the extent possible, a description of the types of personal information that were involved in the data security breach (e.g., full name, SSN, date of birth, home address, account number, disability code, etc.);
- a brief description of what the agency is doing to investigate the breach, to mitigate losses, and to protect against any further breaches;
- contact procedures for those wishing to ask questions or learn additional information, including a toll-free telephone number, website, and/or postal address;
- steps individuals should take to protect themselves from the risk of identity theft (see above for the steps available), including steps to take advantage of any credit monitoring or other service the agency intends to offer and contact information for the FTC website, including specific publications.

Given the amount of information needed to give meaningful notice, an agency may want to consider providing the most important information up front, with the additional details in a Frequently Asked Questions (FAQ) format or on its website. If an agency has knowledge that the affected individuals are not English speaking, notice should also be provided in the appropriate language(s).

4. ***Method of Notification***: Notification should occur in a manner calibrated to ensure that the individuals affected receive actual notice of the incident and the steps they should take. First-class mail notification to the last known mailing address of the individual should be the primary means by which the agency provides notification. Even when an agency has reason to doubt the continued accuracy of such an address or lacks an address, mailed notice may still be effective. The United States Postal Service (USPS) will forward mail to a new address for up to one year, or will provide an updated address via established processes.[12] Moreover, certain agencies, such as the Social Security Administration and the Internal Revenue Service, may sometimes possess address information that can be used to facilitate effective mailing. The notice should be

[12] Agencies may receive updated addresses as a mailer by becoming a direct licensee of the Postal Service or by using a USPS licensed NCOA Link service provider. A current list of service providers is available at http://ribbs.usps.gov/files/ncoalink/CERTIFIED%5FLICENSEES/. For information on address-update and delivery-validation services, contact the USPS at 1-800-589-5766.



sent separately from any other mailing so that it stands out to the recipient. If using another agency to facilitate mailing as referenced above, agencies should take care that the agency that suffered the loss is identified as the sender, not the facilitating agency.

Substitute means of notice such as broad public announcement through the media, website announcements, and distribution to public service and other membership organizations likely to have access to the affected individual class, should be employed to supplement direct mail notification or if the agency cannot obtain a valid mailing address. Email notification is discouraged, as the affected individuals could encounter difficulties in distinguishing the agency's email from a "phishing" email.

The agency also should give special consideration in providing notice to individuals who are visually or hearing impaired consistent with Section 504 of the Rehabilitation Act of 1973. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large-type notice on the agency's web site.

5. ***Preparing for follow-on inquiries***: Those notified can experience considerable frustration if, in the wake of an initial public announcement, they are unable to find sources of additional accurate information. Agencies should be aware that the GSA has a stand-by capability through its "USA Services" operation to quickly put in place a 1-800-FedInfo call center staffed by trained personnel and capable of handling individual inquiries for circumstances in which the number of inquiries is likely to exceed the agency's native capacity. Thus, agencies may wish to consider briefly delaying a public announcement to allow them to implement a consolidated announcement strategy, as opposed to a hasty public announcement without any detailed guidance on steps to take. Such a strategy will permit public statements, website postings, and a call center staffed with individuals prepared to answer the most frequently asked questions all to be made simultaneously available.

6. ***Prepare counterpart entities that may receive a surge in inquiries***: Depending on the nature of the incident, certain entities, such as the credit-reporting agencies or the FTC, may experience a surge in inquiries also. For example, in incidents involving a substantial number of SSNs (e.g., more than 10,000), notifying the three major credit bureaus allows them to prepare to respond to requests from the affected individuals for fraud alerts and/or their credit reports. Thus, especially for large incidents, an agency should inform the credit bureaus and the FTC of the timing and distribution of any notices, as well as the number of affected individuals, in order to prepare.

APPENDIX B

Proposed Routine Use Language

Subsection (b)(3) of the Privacy Act provides that information from an agency's system of records may be disclosed without a subject individual's consent if the disclosure is "for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section." 5 U.S.C. § 552a(b)(3). Subsection (a)(7) of the Act states that "the term 'routine use' means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected." 5 U.S.C. § 552a(a)(7). The Office of Management and Budget, which pursuant to subsection (v) of the Privacy Act has guidance and oversight responsibility for the implementation of the Act by federal agencies, has advised that the compatibility concept encompasses (1) functionally equivalent uses, and (2) other uses that are necessary and proper. 52 Fed. Reg. 12,990, 12,993 (Apr. 20, 1987). In recognition of and in accordance with the Act's legislative history, OMB in its initial Privacy Act guidance stated that "[t]he term routine use . . . recognizes that there are corollary purposes 'compatible with the purpose for which [the information] was collected' that are appropriate and necessary for the efficient conduct of government and in the best interest of both the individual and the public." 40 Fed. Reg. 28,948, 28,953 (July 9, 1975). A routine use to provide for disclosure in connection with response and remedial efforts in the event of a breach of federal data would certainly qualify as such a necessary and proper use of information—a use that is in the best interest of both the individual and the public.

Subsection (e)(4)(D) of the Privacy Act requires that agencies publish notification in the Federal Register of "each routine use of the records contained in the system, including the categories of users and the purpose of such use." 5 U.S.C. § 552a(e)(4)(D). The Department of Justice has developed the following routine use that it plans to apply to its Privacy Act systems of records, and which allows for disclosure as follows:[80]

> To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Agencies should already have a published system of records notice for each of their Privacy Act systems of records. To add a new routine use to an agency's existing systems of records, an agency must simply publish a notice in the Federal Register amending its existing systems of records to include the new routine use.

Subsection (e)(11) of the Privacy Act requires that agencies publish a Federal Register notice of any new routine use at least 30 days prior to its use and "provide an opportunity for interested persons to submit written data, views, or arguments to the agency." 5 U.S.C. § 552a(e)(11). Additionally, subsection (r) of the Act requires that an agency provide Congress and OMB with "adequate advance notice" of any proposal to make a "significant change in a system of records." 5 U.S.C. § 552a(r). OMB has stated that the addition of a routine use qualifies as a significant change that must be reported to Congress and OMB and that such notice is to be provided at least 40 days prior to the alteration. *See* Appendix I to OMB Circular No. A-130—Federal Agency Responsibilities for Maintaining Records About Individuals, 61 Fed. Reg. 6435, 6437 (Feb. 20, 1996). Once a notice is prepared for publication, the agency would send it to the Federal Register, OMB, and Congress, usually simultaneously, and the proposed change to the system (i.e., the new routine use) would become effective 40 days thereafter. *See id*. at 6438 (regarding timing of systems of records reports and noting that notice and comment period for routine uses and period for OMB and congressional review may run concurrently). Recognizing that each agency likely will receive different types of comments in response to its notice, the Task Force recommends that OMB work to ensure accuracy and consistency across the range of agency responses to public comments.

APPENDIX C

Text of Amendments to 18 U.S.C. §§ 3663(b) and 3663A(b)

Proposed Language:

(a) Section 3663 of Title 18, United States Code, is amended by:

(1) Deleting "and" at the end of paragraph (4) of subsection (b);

(2) Deleting the period at the end of paragraph (5) of subsection (b) and inserting in lieu thereof "; and"; and

(3) Adding the following after paragraph (5) of subsection (b):

"(6) in the case of an offense under sections 1028(a)(7) or 1028A(a) of this title, pay an amount equal to the value of the victim's time reasonably spent in an attempt to remediate intended or actual harm incurred from the offense.".

Make conforming changes to the following:

(b) Section 3663A of Title 18, United States Code, is amended by:

(1) Adding the following after Section 3663A(b)(4)

"(5) in the case of an offense under this title, section 1028(a)(7) or 1028A(a), pay an amount equal to the value of the victim's time reasonably spent in an attempt to remediate intended or actual harm incurred from the offense.".

Section Analysis

These new subsections provide that defendants may be ordered to pay restitution to victims of identity theft and aggravated identity theft for the value of the victim's time spent remediating the actual or intended harm of the offense. Restitution could therefore include an amount equal to the value of the victim's time spent clearing a victim's credit report or resolving charges made by the perpetrator for which the victim has been made responsible.

New subsections 3663(b)(6) and 3663A(b)(5) of Title 18 would make clear that restitution orders may include an amount equal to the value of the victim's time spent remediating the actual or intended harm of the identity theft or aggravated identity theft offense. The federal courts of appeals have interpreted the existing provisions of Section 3663 in such a way that would likely preclude the recovery of such amounts, absent explicit statutory authorization. For example, in *United States v. Arvanitis*, 902 F.3d 489 (7th Cir. 1990), the court held that restitution ordered for offenses resulting in loss of property must be limited to recovery of property which is the subject of the offenses, and may not include consequential damages. Similarly, in *United States v. Husky*, 924 F.2d 223 (11th Cir. 1991), the Eleventh Circuit held that the list of compensable expenses in a restitution statute is exclusive, and thus the district court did not have the authority to order the defendant to pay restitution to compensate the victim for mental anguish and suffering. Finally, in *United States v. Schinnell*, 80 F.3d 1064 (5th Cir. 1996), the court held that restitution was not allowed for consequential damages involved in determining the amount of loss or in recovering those funds; thus, a victim of wire fraud was not entitled to restitution for accounting fees and costs to reconstruct bank statements for the time period during which the defendant perpetuated the scheme, for the cost of temporary employees to reconstruct monthly bank statements, and for the costs incurred in borrowing funds to replace stolen funds. These new subsections will provide statutory authority for inclusion of amounts equal to the value of the victim's time reasonably spent remediating the harm incurred as a result of the identity theft offense.

APPENDIX D

Text of Amendments to 18 U.S.C. §§ 2703, 2711 and 3127, and Text of New Language for 18 U.S.C. § 3512

The basis for these proposals is set forth in Section III.2 of the strategic plan, which describes coordination with foreign law enforcement.

Proposed Language:

§ 2703. Required disclosure of customer communications or records

(a) **Contents of wire or electronic communications in electronic storage.**—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure ~~by a court with jurisdiction over the offense under investigation~~ ***by a court of competent jurisdiction*** or an equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) **Contents of wire or electronic communications in a remote computing service.**—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure ~~by a court with jurisdiction over the offense under investigation~~ ***by a court of competent jurisdiction*** or equivalent State warrant; ***or***

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(c) **Records concerning electronic communication service or remote computing service.**—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure ~~by a court with jurisdiction over the offense under investigation~~ ***by a court of competent jurisdiction*** or equivalent State warrant;

§ 2711. Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system; and

(3) the term "court of competent jurisdiction" ~~has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation~~ ***means***—

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that–

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or

(iii) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants.

§ 3127. Definitions for chapter

As used in this chapter—

(1) the terms "wire communication", "electronic communication", "electronic communication service", and "contents" have the meanings set forth for such terms in section 2510 of this title;

(2) the term "court of competent jurisdiction" means—

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals ~~having jurisdiction over the offense being investigated~~ *that*~~–~~

> ***(i) has jurisdiction over the offense being investigated;***
>
> ***(ii) is in or for a district in which the provider of electronic communication service is located;***
>
> ***(iii) is in or for a district in which a landlord, custodian, or other person subject to 3124(a) or (b) is located; or***
>
> ***(iv) is acting on a request for foreign assistance pursuant to section 3512 of this title;*** or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;

§ 3512. Foreign requests for assistance in criminal investigations and prosecutions:

(a) Upon application of an attorney for the government, a Federal judge may issue such orders as may be necessary to execute a request from a foreign authority for assistance in the investigation or prosecution of criminal offenses, or in proceedings related to the prosecution of criminal offenses including but not limited to proceedings regarding forfeiture, sentencing, and restitution. Such orders may include the issuance of a search warrant as provided under Rule 41 of the Federal Rules of Criminal Procedure, a warrant or order for contents of stored wire or electronic communications or for records related thereto as provided under 18 U.S.C. § 2703, an order for a pen register or trap and trace device as provided under 18 U.S.C. § 3123, or an order requiring the appearance of a person for the purpose of providing testimony or a statement, or requiring the production of documents or other things, or both.

(b) In response to an application for execution of a request from a foreign authority as described in subsection (a) , a Federal judge may also issue an order appointing a person to direct the taking of testimony or statements or of the production of documents or other things, or both. A person so appointed may be authorized to –

> ***(1) issue orders requiring the appearance of a person, or the production of documents or other things, or both;***
>
> ***(2) administer any necessary oath; and***
>
> ***(3) take testimony or statements and receive documents or other things.***

(c) Except as provided in subsection (d), an application for execution of a request from a foreign authority under this section may be filed –

(1) in the district in which a person who may be required to appear resides or is located or in which the documents or things to be produced are located;

(2) in cases in which the request seeks the appearance of persons or production of documents or things that may be located in multiple districts, in any one of the districts in which such a person, documents or things may be located; or

(3) in any case, the district in which a related Federal criminal investigation or prosecution is being conducted, or in the District of Columbia.

(d) An application for a search warrant under this section, other than an application for a warrant issued as provided under 18 U.S.C. § 2703, must be filed in the district in which the place or person to be searched is located.

(e) A search warrant may be issued under this section only if the foreign offense for which the evidence is sought involves conduct that, if committed in the United States, would be considered an offense punishable by imprisonment for more than one year under federal or state law.

(f) Except as provided in subsection (d), an order or warrant issued pursuant to this section may be served or executed in any place in the United States.

(g) This section does not preclude any foreign authority or an interested person from obtaining assistance in a criminal investigation or prosecution pursuant to 28 U.S.C. § 1782.

(h) As used in this section –

(1) the term "foreign authority" means a foreign judicial authority, a foreign authority responsible for the investigation or prosecution of criminal offenses or for proceedings related to the prosecution of criminal offenses, or an authority designated as a competent authority or central authority for the purpose of making requests for assistance pursuant to an agreement or treaty with the United States regarding assistance in criminal matters; and

(2) the terms "Federal judge" and "attorney for the Government" have the meaning given such terms for the purposes of the Federal Rules of Criminal Procedure.

APPENDIX E

Text of Amendments to 18 U.S.C. §§ 1028 and 1028A

The basis for these proposed amendments is set forth in Section III.D.4.a of the strategic plan, which describes gaps in the identity theft statutes.

Proposed Amendment to Aggravated Identity Theft Statute to Add Predicate Offenses

Congress should amend the aggravated identity theft offense (18 U.S.C. § 1028A) to include other federal offenses that recur in various identity-theft and fraud cases, specifically, mail theft (18 U.S.C. § 1708), uttering counterfeit securities (18 U.S.C. § 513), and tax fraud (26 U.S.C. §§ 7201, 7206, and 7207), as well as conspiracy to commit specified felonies already listed in section 1028A—in the statutory list of predicate offenses for that offense (18 U.S.C. § 1028A(c)).

Proposed Additions to Both Statutes to Include Misuse of Identifying Information of Organizations

(a) Section 1028(a) of Title 18, United States Code, is amended by inserting in paragraph (7) the phrase "(including an organization as defined in Section 18 of this Title)" after the word "person".

Section 1028A(a) of Title 18, United States Code, is amended by inserting in paragraph (1) the phrase "(including an organization as defined in Section 18 of this Title)" after the word "person".

(b) Section 1028(d)(7) of Title 18, United States Code, is amended by inserting in paragraph (7) the phrase "or other person" after the word "individual".

Rationale:

Corporate identity theft whereby criminals assume the identity of corporate entities to cloak fraudulent schemes in a misleading and deceptive air of legitimacy have become rampant. Criminals routinely engage in unauthorized "appropriation" of legitimate companies' names and logos in a variety of contexts: misrepresenting themselves as officers or employees of a corporation, sending forged or counterfeit documents or financial instruments to victims to improve their aura of legitimacy, and offering nonexistent benefits (e.g., loans and credit cards) in the names of companies.

One egregious example of corporate identity theft is represented on the Internet by the practice commonly known as "phishing," whereby criminals electronically assume the identity of a corporation in order to defraud unsuspecting recipients of email solicitations to voluntarily disclose identifying and financial account information. This personal information is then used to further the underlying criminal scheme—for example, to scavenge the bank and credit card accounts of these unwitting consumer victims. Phishing is just one example of how criminals in mass-marketing fraud schemes incorporate corporate identity theft into their schemes, though phishing also is designed with individual identity theft in mind.

Phishing has become so routine in many major fraud schemes that no particular corporation can be easily singled out as having suffered a special "horror story" which stands above the rest. In August 2005, the "Anti-Phishing Working Group" determined in just that month alone, there were 5,259 unique phishing websites around the world. By December 2005, that number had increased to 7,197, and there were 15,244 unique phishing reports. It was also reported in August 2005, that 84 corporate entities' names (and even logos and web content) were "hijacked" (i.e., misused) in phishing attacks, though only 3 of these corporate brands accounted for 80 percent of phishing campaigns. By December 2005 the number of victimized corporate entities had increased to 120. The financial sector is and has been the most heavily targeted industry sector in phishing schemes, accounting for nearly 85 percent of all phishing attacks. *See, e.g.* ***http://antiphishing.org/apwg_phishing_activity_report_august_05.pdf***.

In addition, major companies have reported to the Department of Justice that their corporate names, logos, and marks are often being misused in other types of fraud schemes. These include telemarketing fraud schemes in which communications purport to come from legitimate banks or companies or offer products or services from legitimate banks and companies, and West African fraud schemes that misuse legitimate banks and companies' names in communications with victims or in counterfeit checks.

Uncertainty has arisen as to whether Congress intended Sections 1028(a)(7) and 1028A(a) of Title 18, United States Code to apply only to "natural" persons or to also protect corporate entities. These two amendments would clarify that Congress intended that these statute apply broadly and may be used against phishing directed against victim corporate entities.

APPENDIX F

Text of Amendment to 18 U.S.C. § 1030(a)(2)

The basis for this proposed amendment is set forth in Section III.D.4.b of the strategic plan, which describes gaps in the computer-related identity theft statutes.

Proposed Language:

1030(a) Whoever—

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains–

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer ~~if the conduct involved an interstate or foreign communication~~;

APPENDIX G

Text of Amendments to 18 U.S.C. §§ 1030(a)(5), (c), and (g), and to 18 U.S.C. § 2332b

The basis for these proposed amendments is set forth in Section III.D.4.b of the strategic plan, which describes gaps in the computer-related identity theft statutes.

Proposed Language:

18 U.S.C. § 1030

(a) Whoever—

(5)

(A) ~~(i)~~ knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) ~~(ii)~~ intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) ~~(iii)~~ intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; ~~and~~

~~(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—~~

~~(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;~~

~~(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;~~

~~(iii) physical injury to any person;~~

~~(iv) a threat to public health or safety; or~~

~~(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;~~

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(2) (A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), ~~(a)(5)(A)(iii)~~, or (a)(6) of this

section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3) ...(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), ~~(a)(5)(A)(iii)~~, or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

~~(4) (A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;~~

~~(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;~~

~~(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and~~

~~(5) (A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and~~

~~(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.~~

(4) (A) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety;

(v) damage affecting a computer used by or for a government entity in furtherance of the administration of justice, national defense, or national security; or

(vi) damage affecting ten or more protected computers during any 1-year period;

or an attempt to commit an offense punishable under this subparagraph;

(B) except as provided in subparagraphs (c)(4)(D) and (c)(4)(E), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subparagraphs (c)(4)(A)(i) through (vi), or an attempt to commit an offense punishable under this subparagraph;

(C) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5) that occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(D) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title or imprisonment for not more than 20 years, or both;

(E) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title or imprisonment for any term of years or for life, or both; or

(F) a fine under this title, imprisonment for not more than one year, or both, for any other offense under subsection (a)(5), or an attempt to commit an offense punishable under this subparagraph.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) ~~of subsection (a)(5)(B)~~ ***subparagraph (c)(4)(A)***. Damages for a violation involving only conduct described in ~~subsection (a)(5)(B)(i)~~ ***subparagraph (c)(4)(A)(i)*** are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

18 U.S.C. § 2332b(g)(5)(B)(I)

...1030(a)(5)(A)~~(i)~~ resulting in damage as defined in ~~1030(a)(5)(B)(ii) through (v)~~ ***1030(c)(4)(A)(ii) through (vi)*** (relating to protection of computers)...

APPENDIX H

Text of Amendments to 18 U.S.C. § 1030(a)(7)

The basis for this proposed amendment is set forth in Section III.D.4.c of the strategic plan, which describes gaps in the cyber-extortion statute.

Proposed Language:

18 U.S.C. § 1030(a)(7)

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any –

(a) threat to cause damage to a protected computer***;***

(b) ***threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or***

(c) ***demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;***

APPENDIX I

Text of Amendment to United States Sentencing Guideline § 2B1.1

The basis for this proposed amendment is set forth in Section III.D.4.d of the strategic plan, which describes the Sentencing Guidelines provision governing identity theft.

Proposed language for United States Sentencing Guidelines § 2B1.1, comment.(n.1):

"Victim" means (A) any person who sustained any harm, whether monetary or non-monetary, as a result of the offense. Harm is intended to be an inclusive term, and includes bodily injury, non-monetary loss such as the theft of a means of identification, invasion of privacy, reputational damage, and inconvenience. "Person" includes individuals, corporations, companies, associations, firms, partnerships, societies, and joint stock companies.

APPENDIX J

Description of Proposed Surveys

In order to expand law enforcement knowledge of the identity theft response and prevention activities of state and local police, the Bureau of Justice Statistics (BJS) should undertake new data collections in three areas: (1) a survey of law enforcement agencies focused on the response to identity theft; (2) enhancements to the existing Law Enforcement Management and Administrative Statistics (LEMAS) survey platform; and (3) enhancements to the existing training academy survey platform. Specifically, BJS should undertake to do the following:

- **New survey of state and local law enforcement agencies.** A new study focused on state and local law enforcement responses to identity theft should seek to document agency personnel, operations, workload, and policies and programs related to the handling of this crime. Detail on the organizational structure, if any, associated with identity theft response should be included (for example, the use of special units devoted to identity theft). The study should inquire about participation in regional identity theft task forces, community outreach and education efforts, as well as identity theft prevention programs. Information collected should also include several summary measures of identity theft in the agencies' jurisdictions (offenses known, arrests, referrals, outcomes), with the goal of producing some standardized metrics with which to compare jurisdictions.
- **Enhancement to existing LEMAS survey.** BJS should develop a special battery of questions for the existing LEMAS survey platform. The LEMAS survey, conducted roughly every three years since 1987, collects detailed administrative information from a nationally representative sample of about 3,000 agencies. The sample includes all agencies with 100 or more officers, and a stratified random sample of smaller agencies as well as campus law enforcement agencies. Information collected should include whether agencies presently enforce identity theft laws, utilize special units, have designated personnel, participate in regional identity theft task forces, and have policies and procedures in place related to the processing of identity theft incidents. The survey should also inquire whether agencies collect summary measures of identity theft in their jurisdictions, including offenses known, arrests, referrals, and any outcome measures. Finally, this study should also collect information on whether agencies are engaged in community outreach, education, and prevention activities related to identity theft.
- **Enhancement to existing law enforcement training academy survey.** BJS should develop a special battery of questions for the existing law enforcement training academy survey platform. A section of the data collection instrument should be devoted to the types of training, if any,

being provided by basic academies across the country in the area of identity theft. BJS should subsequently provide statistics on the number of recruits who receive training on identity theft, as well as the nature and content of the training. In-service training provided to active-duty officers should also be covered.

- **The Bureau of Justice Statistics should revise both the State Court Processing Statistics (SCPS) and National Judicial Reporting Program (NJRP) programs so that they are capable of distinguishing identity theft from other felony offenses.** In addition, the scope of these surveys should be expanded to include misdemeanor identity theft offenders. If SCPS and NJRP were able to follow identity theft offenders, then a variety of different types of court-specific information could be collected. These include how many offenders are charged with identity theft in the Nation's courts, what percentage of these offenders are released at pretrial, and how are the courts adjudicating (e.g., convicting or dismissing) identity theft offenders. Among those convicted identity theft offenders, data should be collected on how many are being sentenced to prison, jail, or probation. These projects should also illuminate the prior criminal histories or rap sheets of identity theft offenders. Both projects should also allow for the post conviction tracking of identity theft offenders for the purposes of examining their overall recidivism rates.
- BJS should ensure that other state court studies that it funds are reconfigured to analyze the problem of identity theft. For example, State Court Organization (SCO) currently surveys the organizational structure of the Nation's state courts. This survey could be supplemented with additional questionnaires that measure whether special courts similar to gun, drug, or domestic violence courts are being created for identity theft offenders. Also, SCO should examine whether courts are training or funding staff equipped to handle identity theft offenders.
- BJS should ensure that the Civil Justice Survey of State Courts, which examines civil trial litigation in a sample of the Nation's state courts, is broadened to identify and track various civil enforcement procedures and their utilization against identity thieves.

ENDNOTES

1. Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998). The Identity Theft Assumption and Deterrence Act provides an expansive definition of identity theft. It includes the misuse of any identifying information, which could include name, SSN, account number, password, or other information linked to an individual, to commit a violation of federal or state law. The definition thus covers misuse of existing accounts as well as creation of new accounts.

2. The federal financial regulatory agencies include the banking and securities regulators, namely, the Federal Deposit Insurance Corporation, the Federal Reserve Board, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Commodity Futures Trading Commission, and the Securities and Exchange Commission.

3. The public comments are available at ***www.idtheft.gov.***

4. Testimony of John M. Harrison, June 19, 2003, Senate Banking Committee, "The Growing Problem of Identity Theft and its Relationship to the Fair Credit Reporting Act."

5. *See* U.S. Attorney's Office, Western District of Michigan, Press Release (July 5, 2006), available at ***http://www.usdoj.gov/usao/miw/press/JMiller_Others10172006.html***.

6. Javelin Strategy and Research, *2007 Identity Fraud Survey Report: Identity Fraud is Dropping, Continued Vigilance Necessary* (Feb 2007), summary available at ***http://www.javelinstrategy.com***; Bureau of Justice Statistics (DOJ) (2004), available at ***http://www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf***; Gartner, Inc. (2003), available at ***http://www.gartner.com/5_about/press_releases/pr21july2003a.jsp***; FTC 2003 Survey Report (2003), available at ***http://www.consumer.gov/idtheft/pdf/synovate_report.pdf***.

7. *See* Business Software Alliance, *Consumer Confidence in Online Shopping Buoyed by Security Software Protection, BSA Survey Suggests* (Jan. 12, 2006), available at ***http://www.bsacybersafety.com/news/2005-Online-Shopping-Confidence.cfm***.

8. *See* Cyber Security Industry Alliance, *Internet Security Voter Survey* (June 2005) at 9, available at ***https://www.csialliance.org/publications/surveys_and_polls/CSIA_Internet_Security_Survey_June_2005.pdf***.

9. *See* U.S. Attorney's Office, Southern District of Florida, Press Release (July 19, 2006), available at ***http://www.usdoj.gov/usao/fls/PressReleases/060719-01.html***.

10. *See*, *e.g.*, John Leland, *Meth Users, Attuned to Detail, Add Another Habit: ID Theft*, New York Times, July 11, 2006, available at ***http://www.nytimes.com/2006/07/11/us/11meth.html?ex=1153540800&en=7b6c7773afa880be&ei=5070***; Byron Acohido and Jon Swartz, ***Meth addicts' other habit: Online Theft***, USA Today, December 14, 2005, available at ***http://www.usatoday.com/tech/news/internetprivacy/2005-12-14-meth-online-theft_x.htm***.

11. Bob Mims, *Id Theft Is the No. 1 Runaway U.S. Crime*, The Salt Lake Tribune, May 3, 2006, available at 2006 WLNR 7592526.

12. Dennis Tomboy, *Meth Addicts Stealing Mail*, Deseret Morning News, April 28, 2005, ***http://deseretnews.com/dn/view/0,1249,600129714,00.html.***

13. Stephen Mihm, *Dumpster-Diving for Your Identity*, New York Times Magazine, December 21, 2003, available at ***http://www.nytimes.com/2003/12/21/magazine/21IDENTITY.html?ex=1387342800&en=b693eef01223bc3b&ei=5007&partner=USERLAND***.

14. Pub. L. No. 108-159, 117 Stat. 1952.

15. The FACT Act required merchants to comply with this truncation provision within three years of the Act's passage with respect to any cash register or device that was in use before January 1, 2005, and within one year of the Act's passage with respect to any cash register or device that was first put into use on or after January 1, 2005. 15 U.S.C. § 1681c(g)(3).

16. *Overview of Attack Trends*, CERT Coordination Center 2002, available at ***http://www.cert.org/archive/pdf/attack_trends.pdf.***

17. Lanowitz, T., Gartner Research ID Number G00127407: December 1, 2005.

18. *"Vishing" Is Latest Twist In Identity Theft Scam,* Consumer Affairs, July 24, 2006, available at ***http://www.consumeraffairs.com/news04/2006/07/scam_vishing.html***.

19. Fraudsters have recently used pretexting techniques to obtain phone records, *see, e.g.*, Jonathan Krim, *Online Data Gets Personal: Cell Phone Records For Sale*, Washington Post, July 13, 2005, available at 2005 WLNR 10979279, and the FTC is pursuing enforcement actions against them. *See* ***http://www.ftc.gov/opa/2006/05/phonerecords.htm***.

20. The FTC brought three cases after sting operations against financial pretexters. Information on the settlement of those cases is available at ***http://www.ftc.gov/opa/2002/03/pretextingsettlements.htm***.

21. *See, e.g.*, *Computers Stolen with Data on 72,000 Medicaid Recipients*, Cincinnati Enquirer, June 3, 2006.

22. 15 U.S.C. § 1681e; 15 U.S.C. § 6802(a).

23. Although the FACT Act amendments to the Fair Credit Reporting Act require merchants to truncate credit account numbers, allowing only the final five digits to appear on an electronically generated receipt, 15 U.S.C. § 1618c(g), manually created receipts might still contain the full account number.

24. *See* ***http://www.bizjournals.com/philadelphia/stories/2006/07/24/daily30.html***. *See also* Identity Theft Resource Center, Fact Sheet 126: *Checking Account Takeover and Check Fraud*, ***http://www.idtheftcenter.org/vg126.shtml***.

25. For example, the Securities and Exchange Commission instituted proceedings against a 19-year-old internet hacker after the hacker illicitly accessed an investor's online brokerage account. His bogus transactions saved the hacker approximately $37,000 in trading losses. The SEC also obtained an emergency asset freeze to halt an Estonia-based "account intrusion" scheme that targeted online brokerage accounts in the U.S. to manipulate the markets. *See* Litigation Release No. 19949 (Dec. 19, 2006), available at ***http://www.sec.gov/litigation/litreleases/2006/lr19949.htm***.

26. For unauthorized credit card charges, the Fair Credit Billing Act limits consumer liability to a maximum of $50 per account. 15 U.S.C. § 1643. For bank account fraud, different laws determine consumers' legal remedies based on the type of fraud that occurred. For example, applicable state laws protect consumers against fraud committed by a thief using paper documents, like stolen or counterfeit checks. If, however, the thief used an electronic fund transfer, federal law applies. The Electronic Fund Transfer Act limits consumer liability for unauthorized transactions involving an ATM or debit card, depending on how quickly the consumer reports the loss or theft of his card: (1) if reported within two business days of discovery, the consumer's losses are limited to a maximum of $50; (2) if reported more than two business days after discovery, but within 60 days of the transmittal date of the account statement containing unauthorized transactions, he could lose up to $500; and (3) if reported more than 60 days after the transmittal date of the account statement containing unauthorized transactions, he could face unlimited liability. 15 U.S.C. § 1693g. As a matter of policy, some credit and debit card companies waive liability under some circumstances, freeing the consumer from fraudulent use of his credit or debit card.

27. *See* John Leland, *Some ID Theft Is Not For Profit, But to Get a Job*, N.Y. Times, Sept. 4, 2006.

28. *See* World Privacy Forum, *Medical Identity Theft: The Information Crime That Can Kill You* (May 3, 2006), available at ***worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf***.

29. *See* ***http://www.idanalytics.com/news_and_events/20051208.htm***. Some other organizations have begun conducting statistical analyses to determine the link between data breaches and identity theft. These efforts are still in their early stages, however.

30. Government Accounting Office, *Social Security Numbers: Government Could Do More to Reduce Display in Public Records and On Identity Cards* (November 2004), at 2, available at ***http://www.gao.gov/new.items/d0559.pdf***.

31. 15 U.S.C. §§ 6801 et seq.; 42 U.S.C. §§ 1320d et seq.; 18 U.S.C. §§ 2721 et seq.

32. 5 U.S.C. § 552a.

33. *See*, *e.g.*, Ariz. Rev. Stat. § 44-1373.

34. *Social Security Numbers: Federal and State Laws Restrict Use of SSNs, Yet Gaps Remain*, GAO - 05-1016T, September 15, 2005.

35. *See*, *e.g.*, ***www.wpsic.com/edi/comm_sub_p.shtml?mm=3***, *Non-SSN Member Numbers to Be Assigned for Privacy Protection*.

36. Except where expressly noted, all references to years in this strategic plan are intended to refer to calendar years, rather than fiscal years.

37. The federal government's overall information privacy program derives primarily from five statutes that assign OMB policy and oversight responsibilities, and agencies responsibility for implementation. The Privacy Act of 1974 (5 U.S.C. § 552a) sets collection, maintenance, and disclosure conditions; access and amendment rights and notice and record-keeping requirements with respect to personally identifiable information retrieved by name or personal identifier. The Computer Matching and Privacy Protection Act of 1988 (5 U.S.C. § 552a note) amended the Privacy Act to provide a framework for the electronic comparison of personnel and benefits-related information systems. The Paperwork Reduction Act of 1995 (44 U.S.C. § 3501 et seq.) and the Information Technology Management Reform Act of 1996 (also known as Clinger-Cohen Act; 41 U.S.C. § 251 note) linked agency privacy activities to information technology and information resources management, and assigned to agency Chief Information Officers (CIO) the responsibility to ensure implementation of privacy programs within their respective agencies. Finally, Section 208 of the E-Government Act of 2002 (44 U.S.C. § 3501 note) included provisions requiring agencies to conduct privacy impact assessments on new or substantially altered information technology systems and electronic information collections, and post web privacy policies at major entry points to their Internet sites. These provisions are discussed in OMB memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002."

38. *See Protection of Sensitive Agency Information*, Memorandum from Clay Johnson III, Deputy Director for Management, OMB, to Heads of Departments and Agencies, M-06-16 (June 23, 2006).

39. The United States Computer Emergency Readiness Team (US-CERT) has played an important role in public sector data security. US-CERT is a partnership between DHS and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. The organization interacts with federal agencies, state and local governments, industry professionals, and others to improve information sharing and incident response coordination and to reduce cyber threats and vulnerabilities. US-CERT provides the following support: (1) cyber security event monitoring; (2) advanced warning on emerging threats; (3) incident response capabilities for federal and state agencies; (4) malware analysis and recovery support; (5) trends and analysis reporting tools; and (6) other support services in the area of cyber security. US-CERT also provides consumer and business education on Internet and information security.

40. *See* ***http://www.whitehouse.gov/results/agenda/scorecard.html.***

41. The proposed routine use language set forth in Appendix B differs slightly from that included in the Task Force's interim recommendations in that it further clarifies, among other things, the categories of users and the circumstances under which disclosure would be "necessary and proper" in accordance with the OMB's guidance on this issue.

42. 15 U.S.C. §§ 6801-09; 16 C.F.R. Part 313 (FTC); 12 C.F.R. Part 30, App. B (OCC, national banks); 12 C.F.R. Part 208, App. D-2 and Part 225, App. F (FRB, state member banks and holding companies); 12 C.F.R. Part 364, App. B (FDIC, state non-member banks); 12 C.F.R. Part 570, App. B (OTS, savings associations); 12 C.F.R. Part 748, App. A (NCUA, credit unions); 16 C.F.R. Part 314 (FTC, financial institutions that are not regulated by the FRB, FDIC, OCC, OTS, NCUA, CFTC, or SEC); 17 C.F.R. Part 248.30 (SEC); 17 C.F.R. Part 160.30 (CFTC).

43. 15 U.S.C. § 45(a). Further, the federal bank regulatory agencies have authority to enforce Section 5 of the FTC Act against entities over which they have jurisdiction. *See* 15 U.S.C. §§ 6801-09.

44. 15 U.S.C. §§ 1681-1681x, as amended.

45. Pub. L. No. 108-159, 117 Stat. 1952.

46. 42 U.S.C. §§ 1320d et seq.

47. 31 U.S.C. § 5318(l).

48. 18 U.S.C. §§ 2721 et seq.

49. ***http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm***.

50. ***http://www.bbb.org/securityandprivacy/SecurityPrivacyMadeSimpler.pdf***;***www.staysafeonline.org/basics/company/basic_tips.html***;*The Financial Services Roundtable, Voluntary Guidelines for Consumer Confidence in Online Financial Services*, available at ***www.bitsinfo.org/downloads/Publications%20Page/bitsconscon.pdf***; ***www.realtor.org/realtororg.nsf/files/NARInternetSecurityGuide.pdf/$FILE/NARInternetSecurityGuide.pdf***; ***www.antiphishing.org/reports/bestpracticesforisps.pdf***; ***www.uschamber.com/sb/security/default.htm***; ***www.truste.org/pdf/SecurityGuidelines.pdf***; ***www.the-dma.org/privacy/informationsecurity.shtml***; ***http://www.staysafeonline.org/basics/company/basic_tips.html***.

51. These changes may be attributable to requirements contained in the regulations implementing Title V of the GLB Act. *See* 12 C.F.R. Part 30, App. B (national banks); 12 C.F.R. Part 208, App. D-2 and Part 225, App. 5 (state member banks and holding companies); 12 C.F.R. Part 364, App. B (state non-member banks); 12 C.F.R. Part 570, App. B (savings associations); 12 C.F.R. Part 748, App. A and B, and 12 C.F.R. Part 717 (credit unions); 16 C.F.R. Part 314 (financial institutions that are not regulated by the FDIC, FRB, NCUA, OCC, or OTS).

52. *See*, *e.g.*, ***http://www.truste.org/pdf/SecurityGuidelines.pdf***; ***http://www.the-dma.org/privacy/informationsecurity.shtml***.

53. Deloitte Financial Services, *2006 Global Security Survey*, available at ***http://singe.rucus.net/blog/archives/756-Deloitte-Security-Surveys.html.***

54. Datalink, *Data Storage Security Study*, March 2006, available at ***www.datalink.com/security/.***

55. *Id*.

56. *See* Small Business Technology Institute, *Small Business Information Security Readiness* (July 2005).

57. *See*, *e.g.*, California (Cal. Civ. Code § 1798.82 (2006)); Illinois (815 Ill. Comp. Stat 530/5 (2005)); Louisiana (La. Rev. Stat. 51:3074 (2006)); Rhode Island (R.I. Gen. Laws § 11-49.2.3 (2006)).

58. *See*, *e.g.*, Colorado (Colo. Rev. Stat. § 6-1-716 (2006)); Florida (Fla. Stat. § 817.5681 (2005)); New York (NY CLS Gen. Bus. § 889-aa (2006)); Ohio (Ohio Rev. Code Ann. § 1349.19 (2006)).

59. Ponemon Institute LLC, *Benchmark Study of European and U.S. Corporate Privacy Practices*, p. 16 (Apr. 26, 2006).

60. *Id.*

61. Ponemon Institute, LLC, 2005 *Benchmark Study of Corporate Privacy Practices* (July 11, 2005).

62. MultiChannel Merchant, *Retailers Need to Provide Greater Data Security, Survey Says* (Dec. 1, 2005), available at ***http://multichannelmerchant.com/opsandfulfillment/advisor/retailers_data_security_1201/index.html***.

63. *See* Information Technology Examination Handbook's Information Security Booklet, available at ***http://www.ffiec.gov/guides.htm***.

64. *See*, *e.g.*, ***http://www.pvkansas.com/police/crime/iden_theft.shtml*** (Prairie Village, Kansas), ***http://phoenix.gov//POLICE/dcd1.html*** (Phoenix, Arizona); ***www.co.arapahoe.co.us/departments/SH/index.asp*** (Arapahoe County, Colorado).

65. *Colleges Are Textbook Cases of Cybersecurity Breaches*, USA TODAY, August 1, 2006.

66. Examples of this outreach include a wide-scale effort at the University of Michigan which launched Identity Web, a comprehensive site based on the recommendations of a graduate class in fall of 2003. The State University of New York's Orange County Community College offers identity theft seminars, the result of a student who fell victim to a scam. A video at student orientation sessions at Drexel University in Philadelphia warns students of the dangers of identity theft on social networking sites. Bowling Green State University in Kentucky emails campus-wide "fraud alerts" when it suspects that a scam is being targeted to its students. In recent years, more colleges and universities have hired chief privacy officers, focusing greater attention on the harms that can result from the misuse of students' information.

67. *See* 31 C.F.R. § 103.121 (banks, savings associations, credit unions, and certain non-federally regulated banks); 31 C.F.R. § 103.122 (broker-dealers); 17 C.F.R. § 270.0-11, 31 C.F.R. § 103.131 (mutual funds); and 31 C.F.R. § 103.123 (futures commission merchants and introducing brokers).

68. *See* ***http://www.dhs.gov/xprevprot/laws/gc_1172765386179.shtm***.

69. A primary reason criminals use other people's identities to commit identity theft is to enable them to operate with anonymity. However, in committing identity theft, the suspects often leave telltale signs that should trigger concern for alert businesses. Section 114 of the FACT Act seeks to take advantage of businesses' awareness of these patterns, and requires the federal bank regulatory agencies and the FTC to develop regulations and guidelines for financial institutions and creditors addressing identity theft. In developing the guidelines, the agencies must identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft. 15 U.S.C. § 1681m.

    Those agencies have issued a set of proposed regulations that would require each financial institution and creditor to develop and implement an identity theft prevention program that includes policies and procedures for detecting, preventing, and mitigating identity theft in connection with account openings and existing accounts. The proposed regulations include guidelines listing patterns, practices, and specific forms of activity that should raise a "red flag" signaling a possible risk of identity theft. Recognizing these "red flags" can enable businesses to detect identity theft at its early stages before too much harm is done. *See* 71 Fed. Reg. 40786 (July 18, 2006) to be codified at 12 C.F.R. Parts 41 (OCC), 222 (FRB), 334 and 364 (FDIC), 571 (OTS), 717 (NCUA), and 16 C.F.R. Part 681 (FTC), available at ***http://www.occ.gov/fr/fedregister/71fr40786.pdf***.

70. USB token devices are typically small vehicles for storing data. They are difficult to duplicate and are tamper-resistant. The USB token is plugged directly into the USB port of a computer, avoiding the need for any special hardware on the user's computer. However, a login and password are still required to access the information contained on the device. Smart cards resemble a credit card and contain a microprocessor that allows them to store and retain information. Smart cards are inserted into a compatible reader and, if recognized, may require a password to perform a transaction. Finally, the common token system involves a device that generates a one-time password at predetermined intervals. Typically, this password would be used in conjunction with other login information such as a PIN to allow access to a computer network. This system is frequently used to allow for remote access to a work station for a telecommuter.

71. Biometrics are automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics. Biometrics commonly implemented or studied include: fingerprint, face, iris, voice, signature, and hand geometry. Many other modalities are in various stages of development and assessment. Additional information on biometric technologies, federal biometric programs, and associated privacy considerations can be found at ***www.biometrics.gov***.

72. *See Authentication in an Internet Banking Environment* (October 12, 2005), available at ***http://www.ffiec.gov/pdf/authentication_guidance.pdf***.

73. *See* FFIEC Frequently Asked Questions on *FFIEC Guidance on Authentication in an Internet Banking Environment* (August 15, 2006), available at ***http://www.ffiec.gov/pdf/authentication_faq.pdf***.

74. *See* Kristin Davis and Jessica Anderson, *But Officer, That Isn't Me*, Kiplinger's Personal Finance (October 2005); Bob Sullivan, *The Darkest Side of ID Theft*, MSNBC.com (Dec. 1, 2003); David Brietkopf, *State of Va. Creates Special Cards for Crime Victims*, The American Banker (Nov. 18, 2003).

75. 18 U.S.C. § 1028A.

76. 18 U.S.C. § 1028(d)(7).

77. *See* 18 U.S.C. § 1030(e)(8).

78. 18 U.S.C. § 1030(a)(7).

79. S. Rep. No. 105-274, at 9 (1998).

80. As this Task Force has been charged with considering the federal response to identity theft, this routine use notice does not include all possible triggers, such as embarrassment or harm to reputation. However, after consideration of the Strategic Plan and the work of other groups charged with assessing Privacy Act considerations, OMB may determine that a routine use that takes into account other possible triggers may be preferable.

UPDATED
WITH COMPLETE
2008 DATA

Cisco 2008
Annual Security Report

Highlighting global security threats and trends

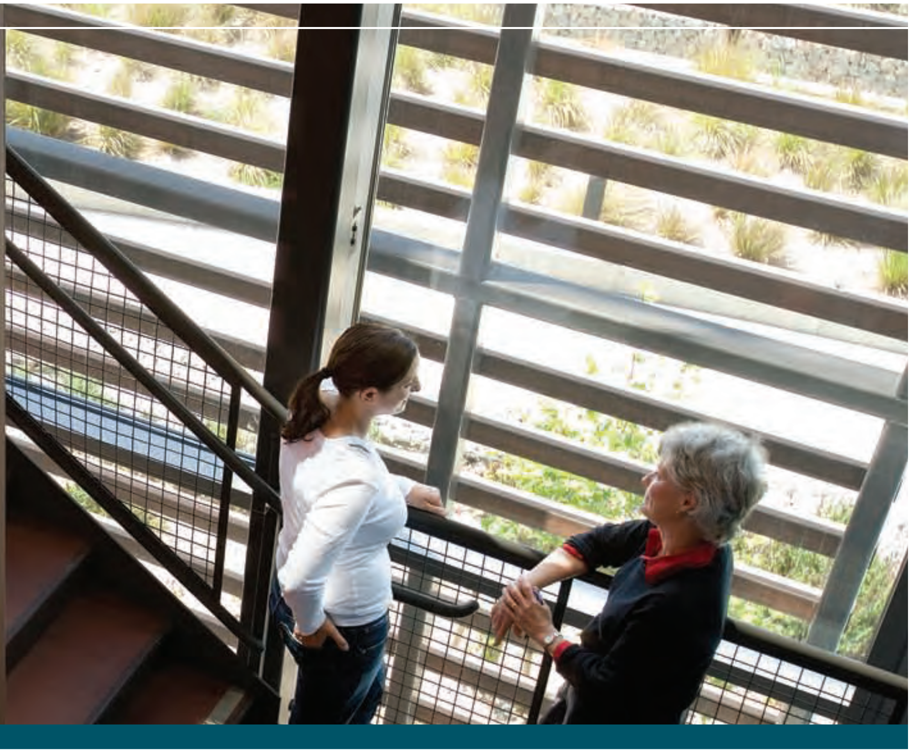
Contents

The Cisco® Annual Security Report provides an overview of the combined security intelligence of the entire Cisco organization. The report encompasses threat information and trends collected between January and December 2008, and provides a snapshot of the state of security for that period. The report also provides recommendations from Cisco security experts and predictions of how identified trends will continue to unfold in 2009.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Introduction



There was an enormous amount of activity related to data and online security during the past year. Although no single, overwhelming attack—such as the spread of Melissa, Slammer, or Storm malware in previous years—turned into the signature security event of 2008, the need for increased security protection and continued vigilance remains.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Compared to previous years, online criminals are becoming even more sophisticated and effective, employing a greater number of relatively smaller, more targeted campaigns to gain access to sensitive data. Human nature—in the forms of insider threats, susceptibility to social engineering, and carelessness that leads to inadvertent data loss—continues to be a major factor in countless security incidents. And the increasing use at many organizations of technologies designed to increase collaboration and productivity (such as mobile devices, virtualization, cloud computing, and other Web-based tools and Web 2.0 applications) is stretching the edges of corporate networks, potentially increasing security risks.

Many different entry points or "threat vectors" are used to compromise the security of individuals and organizations. For example, threats can be aimed at mobile devices and insecure hardware; at weaknesses in operating systems, office productivity applications, and encryption tools; and at numerous other vectors.

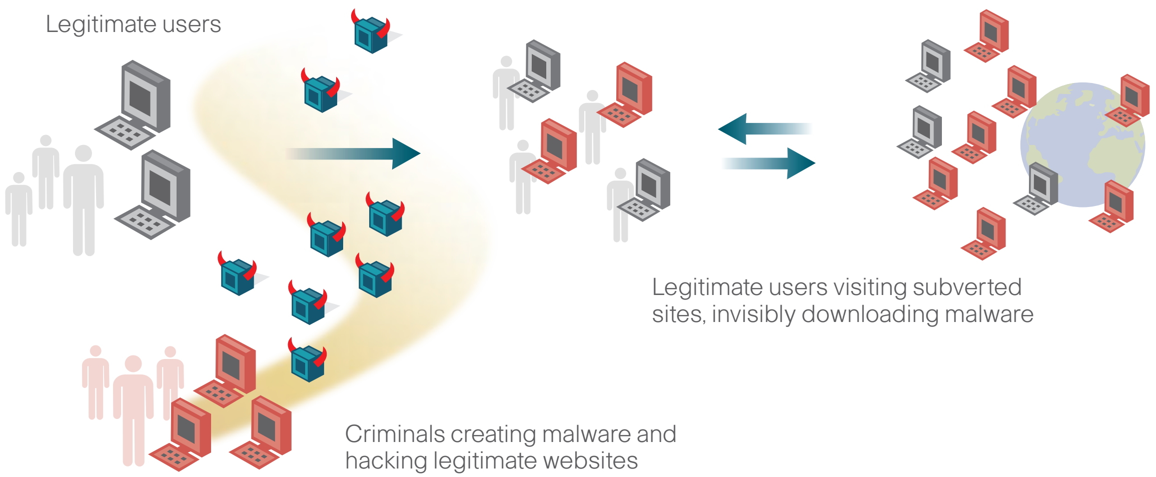
Online Threats

In terms of quantity and pervasiveness, the most significant security threats in 2008 involved an online component. These online threats continue to grow in scope and number, and should remain a top concern for security professionals.

Many of these online threats combine the following closely related elements:

- The World Wide Web
- Malware
- Botnets
- Spam

Online Criminal Ecosystem


Legitimate users
Legitimate users visiting subverted sites, invisibly downloading malware
Criminals creating malware and hacking legitimate websites

The Web

In the online threat arena, the entire Web ecosystem comes into play. Online criminals continue to create malicious websites—carefully designing them to look alluring and legitimate—to obtain sensitive personal information or distribute malware to site visitors. They hack legitimate websites from trusted organizations, such as news media or large retailers, to cause those sites to invisibly distribute malware to visitors; they also create or subvert existing Web applications and plug-ins for the same purpose. In addition, in the core underlying infrastructure of the Internet, weaknesses have been exposed that could let online criminals divert thousands of unsuspecting Internet users at once to malicious websites.

Malware

Although far from the only method, the Web has become the primary means of infecting computers with malicious software. Most modern "malware" is designed to help someone gain control over a computer, communications device, or network. Some malware directly influences or changes an infected computer's activities—for example, causing it to connect to the Internet or install additional malware without the user's knowledge. Other malware works to find sensitive information, such as user passwords and credit card numbers, on a computer or network, and sends that information "home" to online criminals. In addition, an increasing amount of malware is being developed and sold.

Botnets

The core mission for much of today's malware is to infiltrate a computer and make it part of a botnet. Botnets consist of thousands of malware-compromised computers (botnet nodes or "zombies"), and they have become the cornerstone of large-scale online criminal activity. The people controlling botnets can rent out the processing power and bandwidth of these subverted computers to others, or use it themselves to send out massive amounts of spam, attack websites, or engage in other nefarious behavior.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Spam by Originating Country for 2008

Originating Country	Percentage of Global Spam
United States	15.9%
Turkey	7.4%
Russian Federation	7.2%
China	6.1%
Brazil	5.1%
United Kingdom	3.4%
Korea	3.3%
Poland	3.2%
India	3.0%
Italy	3.0%
Germany	3.0%
Spain	2.8%
Argentina	2.5%
Colombia	2.3%
Thailand	2.2%
France	2.0%
Other	27.6%

Spam

Spam, or unsolicited email, is one of the most pervasive Internet threats, affecting nearly every Internet user and organization in the world. Different types of spam include:

- Email messages promoting items such as pharmaceuticals, printer cartridges or corporate equity instruments for sale.
- Email messages with an attached file that contains malware.
- "Phishing" emails that lure recipients into providing personal information via a return email or by filling out forms on a website.
- Email messages that include URLs and attempt to convince recipients to visit seemingly trustworthy websites that actually distribute malware.

Many spammers still blast out "mass-mailing" spam to millions of untargeted recipients per campaign; many anti-spam products work on filtering out these types of messages. But for more sophisticated "phishing" spam—which is designed to elicit personal or financial information—smaller, more targeted campaigns are becoming the norm.

Spammers continue to improve the design and effectiveness of their messages. They're using highly topical subject lines, far more legitimate-looking and professional-sounding content, and other techniques that make certain types of spam hard to resist for normally wary recipients—and easier to slip by anti-spam solutions.

To actually send out their spam messages, online criminals rarely use computers in their physical possession, instead renting or building botnets to do the mailing for them. This completes an elegant cycle, in which:

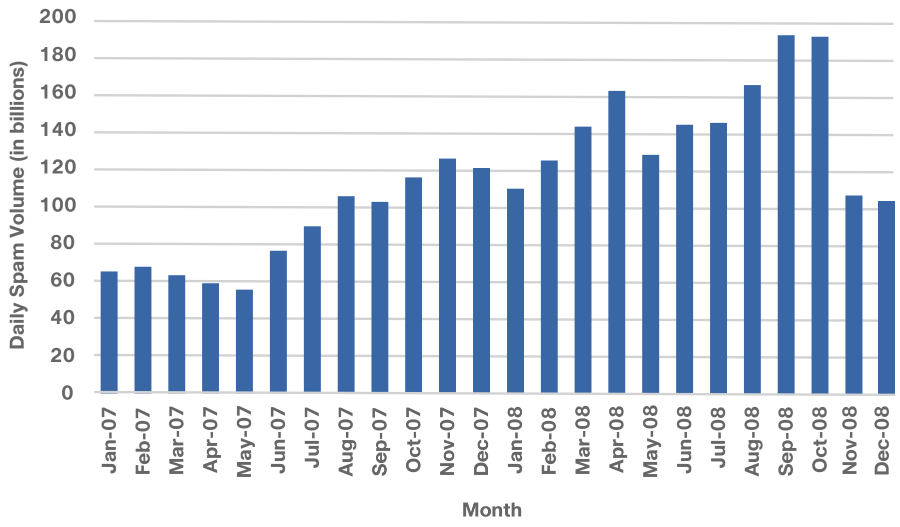
- Botnet nodes send out spam.
- Spam recipients get an email message that lures them to a malicious website.
- The website downloads malware onto the site visitor's computer to gain control over it.
- The compromised computer becomes part of a botnet, and starts sending out spam.

Data Loss

Data loss often occurs through the loss or theft of equipment such as laptops or removable storage media, or when a computer or network is infiltrated to steal sensitive data or intellectual property. Fewer organizations and individuals may be affected by data loss incidents than by online threats, but the impact of these events can be devastating.

For organizations that experience data loss, reputations and trust can be damaged or destroyed, while financial consequences such as stock-price drops, lawsuits, and compensatory damages to affected individuals can run into millions or even billions of dollars. For individuals, the consequences of a data loss incident that compromises highly personal information, such as Social Security numbers or financial details, can negatively affect their lives and finances for years.

Average Daily Spam Volume



Daily spam volumes have nearly doubled in 2008 relative to 2007.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Legislation and industry initiatives focused on making data on networks more secure and informing parties affected of data breaches are increasing. Many organizations are working to better enforce their existing acceptable use policies around sensitive data. Yet compliance with such policies and initiatives is not a guarantee of safety, as the growth and evolution of data loss threat factors are likely to outpace the initiatives or legislation addressing them.

Insider Threats

Sometimes, the people responsible for data loss and other security incidents are insiders, including current or former employees who want to cause trouble or are simply looking for personal gain. This type of threat can be especially grave, as insiders know the weaknesses in an organization's security and how best to exploit them to steal data or money, or even hold assets for ransom. In today's uncertain economy, in which more employees may lose their jobs or become dissatisfied with their work situation, and in which less budget may be available to address security concerns, insider threats —and the likelihood of their success—are of increasing concern.

Vulnerabilities

In addition to taking advantage of aspects of human nature (such as curiosity, trust, and carelessness), criminals are getting access to computers and networks by exploiting weaknesses in technologies, software, and systems.

In 2008, vulnerabilities in the entire Web ecosystem—browsers; helper objects, media players, and plug-ins running in those browsers; Web server and application software; and core parts of the underlying infrastructure of the Web—were exploited to gain control of computers, networks, and data.

Top Security Concerns of 2008

Threats and criminals are becoming faster, smarter, and more covert.

- Specialization and innovation in the online crime economy continues.
- Attacks are increasingly targeted to help maximize their effectiveness.
- Many types of reputation hijacking (attacks that exploit users' trust in someone's reputation) are gaining in prevalence and popularity.
- Blended threats that combine email and websites and use social engineering techniques are now more common than ever.

Criminals are exploiting vulnerabilities along the entire Web ecosystem to gain control of computers and networks.

- Botnet infestations remain common and dangerous.
- Known vulnerabilities are going unpatched and existing security policies are being ignored.
- Widespread use of Web-based collaborative technologies in the workplace brings added risks as well as greater productivity.

"Invisible threats" (such as hard-to-detect infections of legitimate websites) are making common sense and many traditional security solutions ineffective.

Loss of data and intellectual property are continual challenges.

- Data loss is often caused by exploiting vulnerabilities in technology and human nature.
- A company's reputation, trust and finances can be affected.
- Risk vectors include online threats, mobile devices, and insiders.

Other vulnerabilities can be exploited as well, including (among others) weaknesses in office productivity applications, operating systems, mobile device technologies, networking equipment, virtualization tools, and encryption technologies. However, vendors of affected products are now often disclosing vulnerabilities—and releasing patches at the same time—to mitigate the effects of the vulnerability, making staying up-to-date on patches more important than ever.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Online Security Risks and Trends

Online security threats continued their growth in 2008. Online criminals combined spam, phishing, botnets, malware, and malicious or compromised websites to create highly effective blended threats that use multiple online vectors to defraud and compromise the security of Internet users.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

The Web itself is a primary mechanism for distributing malware that lets someone gain control over computers and networks. Many of these computers are then turned into nodes in a botnet, where they engage in a variety of activities, usually without the computer user ever being aware that this is happening.

These activities can include sending massive volumes of spam—designed to either lure more victims to websites where they'll download malware, or to obtain personal information—hosting malicious websites or infecting legitimate websites, and helping to overwhelm websites or computer networks with distributed denial of service (DDoS) attacks.

Web Trends

Fifteen years ago, barely anyone knew what the World Wide Web was. Today, Google is one of the top trusted brands in the world, and people extensively use the Web for everyday activities such as communication, research, shopping, and financial matters.

Unlike its earliest predecessors, the modern Web browser provides an amazing, highly interactive experience. Flash animation ads play within a webpage; audio streams on the websites of bands or online radio stations let site visitors listen to music; videos play automatically; social networking sites and widgets integrate contact information, photos, or data from a person's blog with their social networking page; and Adobe PDF documents render seamlessly within the browser.

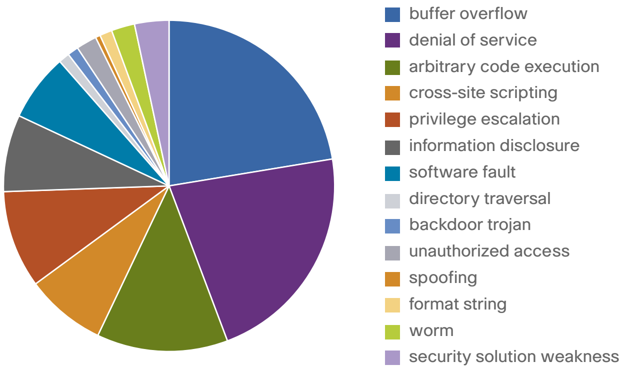
This is all possible because the Web browser uses plug-ins, media players, browser helper objects, and tools like ActiveX controls and JavaScript commands to activate different types of objects on a webpage. Underlying Web applications such as content management systems show the right content at the right time, while forums and wikis let site visitors quickly post to and modify webpages.

As the possibilities and popularity of the Web have grown, so has its use as a threat vector.

Originally, malicious software was distributed via floppy drives and macros in infected office documents, then via network worms such as Slammer, followed by an enormous rise in distribution via email. Today, a vast quantity of malware is downloaded from websites. Criminals exploit vulnerabilities throughout the entire Web ecosystem to gain control of computers and networks. (For more specific examples and information, see the *Vulnerabilities* section later in this report.)

These malware infections often happen without any user intervention or awareness in what is known as a "drive-by download." Someone visits a malicious or infected website hosting exploits that look for weaknesses in the site visitor's browser or computer system. If the exploits detect a usable weakness, they start trying to download malware to the computer. This can all happen quietly in the background, without the site visitor ever clicking on a link in the infected page or finding out what's going on.

Vulnerability and Threat Categories for 2008



In 2008, vulnerability and threat activity was dominated by buffer overflows and denials of service, with arbitrary code execution being the next most prominent category.

More and more of these malicious websites involve "in-depth" attacks, where several different types of exploits that work on different weaknesses (in different browsers, plug-ins, and operating systems) are hosted on the same website. This increases the chance that each website visitor will display a weakness—and one is all that's needed—that the exploits can take advantage of to download malware to the computer.

Compromising Legitimate Websites

A method of propagating malware that reached new levels of popularity in 2008 is compromising legitimate websites to make them hubs for malware distribution. In April 2008 alone, thousands of websites were compromised and tried to infect site visitors with malware.

Causing a trusted legitimate website to host exploits or serve up malicious code is an effective way to infect computers with malware. Site visitors have no hesitation about the trustworthiness of the site; it is a legitimate site they visit for content or transactions on a regular basis. Internet security applications that depend on URL or IP address filtering also trust the website's legitimacy.

And when legitimate websites are infected, specific user groups can be targeted with great precision—for example, infecting sites aimed at students, online gamers, or business users, with the latter potentially providing channels into business networks through compromised workplace computers.

Cisco data shows that exploited websites are currently responsible for more than 87 percent of all Web-based threats. And according to security audit provider White Hat Security, more than 79 percent of the websites hosting malicious code are *legitimate* websites that have been compromised. Nine out of any 10 websites may be vulnerable to attack: Seven out of 10 are susceptible to cross-site scripting (XSS) exploits, and one in every five may be vulnerable to SQL injection attacks.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

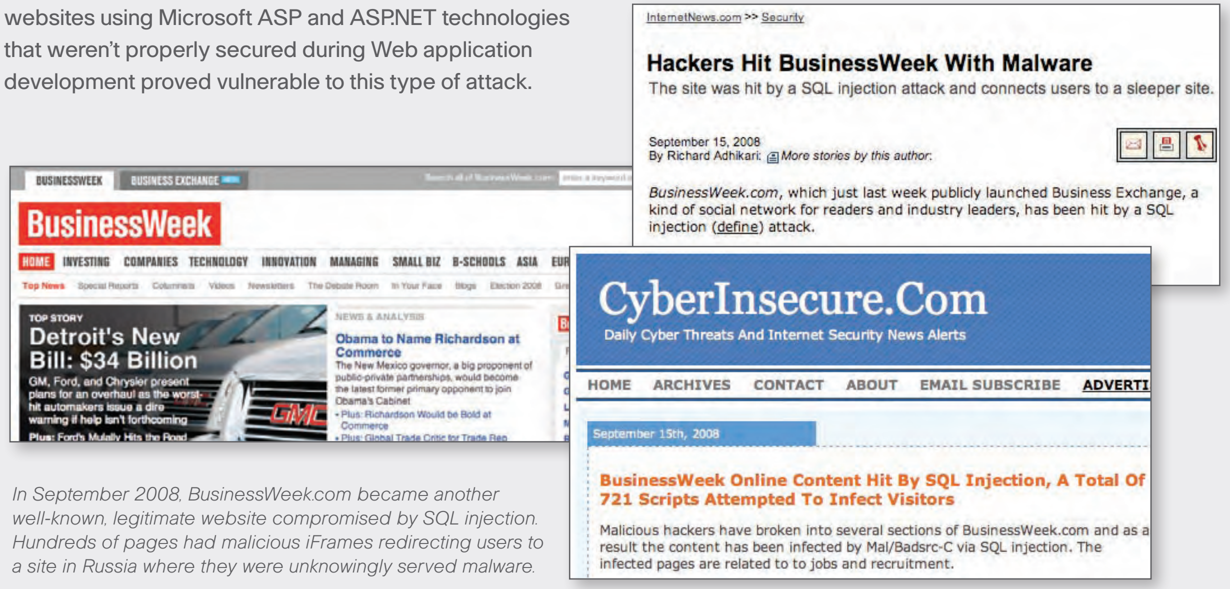
Popular Methods of Compromising Legitimate Websites

iFrame exploits. Both XSS and SQL injection exploits commonly use iFrames as a vehicle for delivering malicious code, which can install malware on a computer without the user's knowledge. An iFrame, or inline frame HTML tag, can allow the embedding of compromised Web code from another Web server into a separate HTML document. Common applications of this method include setting the size of the iFrame to zero and simply passing malicious code through the host site without the knowledge of the site visitor or the Web host.

SQL injection. Exploits a security vulnerability in the database layer of widely used Web applications and servers. Recently, hackers have used Structured Query Language (SQL) exploits to include malware or invisible links to malware-hosting sites on legitimate websites. They did this by taking advantage of website developers not properly sanitizing data transmitted in user input fields (such as forms and user logins) on webpages that use SQL. Thousands of websites using Microsoft ASP and ASP.NET technologies that weren't properly secured during Web application development proved vulnerable to this type of attack.

Cross-site scripting (XSS). A flaw within Web applications that lets ill-intentioned users of vulnerable websites or owners of malicious websites send malicious code to the browsers of unsuspecting users. These attacks are frequently executed using HTML image and frame elements (<img>, <frame>, <iframe>) and JavaScript.

Cross-site request forgery (CSRF or XSRF). An exploit in which an attacker uses the knowledge that the victim is currently engaged in a browser session on one website to forge instructions ostensibly from the victim on another site where the user is persistently or currently authenticated. For example, the attacker and victim are both online in a Web forum, and the attacker is able to steal the victim's authentication to make purchases at an e-commerce site that the attacker knows a) is frequented by the victim, and b) does not require re-authentication before finalizing purchases.



Hackers Hit BusinessWeek With Malware

The site was hit by a SQL injection attack and connects users to a sleeper site.

September 15, 2008
By Richard Adhikari: More stories by this author:

BusinessWeek.com, which just last week publicly launched Business Exchange, a kind of social network for readers and industry leaders, has been hit by a SQL injection (define) attack.

Detroit's New Bill: $34 Billion

GM, Ford, and Chrysler present plans for an overhaul as the worst-hit automakers issue a dire warning if help isn't forthcoming

Plus: Ford's Mulally Hits the Road

Obama to Name Richardson at Commerce

The New Mexico governor, a big proponent of public-private partnerships, would become the latest former primary opponent to join Obama's Cabinet

- Plus: Richardson Would be Bold at Commerce
- Plus: Global Trade Critic for Trade Rep

September 15th, 2008

BusinessWeek Online Content Hit By SQL Injection, A Total Of 721 Scripts Attempted To Infect Visitors

Malicious hackers have broken into several sections of BusinessWeek.com and as a result the content has been infected by Mal/Badsrc-C via SQL injection. The infected pages are related to to jobs and recruitment.

In September 2008, BusinessWeek.com became another well-known, legitimate website compromised by SQL injection. Hundreds of pages had malicious iFrames redirecting users to a site in Russia where they were unknowingly served malware.

In one notorious case in September 2008, online criminals compromised hundreds of pages on the BusinessWeek.com website with a SQL injection attack. As one of the top 1000 visited sites on the Web, BusinessWeek.com enjoys a high degree of trust from Web users. Naturally, that makes it extraordinarily attractive as a site from which to serve malware to unsuspecting visitors.

Malware Trends

A vast amount of online crime and profit is enabled by control of personal computers. The malware, or malicious software that infects these computers and turns them into botnet nodes, is the first step.

2008 was another banner year for Web-based malware. Online criminals continued employing the Web-based distribution techniques that worked so well for them in 2007, and kept refining them further for greater effectiveness and profit.

Of the malware distributed via the Web, a large portion consisted of Trojans, designed to seem innocuous, invisible, or attractive before being installed. Rootkits, which help downloaded malware stay hidden, were also prevalent. Other widely distributed malware included spyware and keyloggers, both of which send information about a compromised user's computing and Web surfing habits and personal information—including passwords—back to the malware distributors.

The volume of malware successfully propagated via email attachments has declined in recent years. This decline could be related to Web-based malware distribution methods proving so effective, and to the ability of anti-malware products to rapidly detect and block much of the email that contains malware. These factors may have led malware creators to spend more time on malware spread via the Web rather than via email.

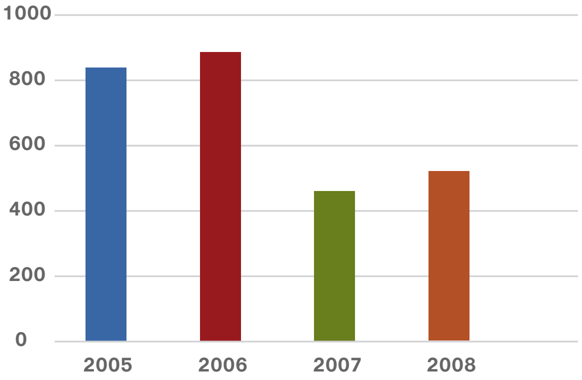
All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Of the attachment-based malware campaigns of 2008, popular ones included messages claiming to contain delivery forms from UPS or FedEx, or messages claiming their attachment was an invoice, an e-ticket, an e-card (from Hallmark, for example), or video or pictures that were actually executable files.

Another attachment-based malware campaign shut down the IT systems of three British hospitals, when the hospitals' computer networks became infected with email-propagated Mytob malware.

To prosper, malware creators must develop tools that are tough for anti-malware solutions to detect; they are building more surreptitious malware designed to avoid detection by anti-virus and anti-malware programs. One popular technique is malware that can temporarily go dormant. Another is malware code that continually and automatically changes just enough to confuse signature-based anti-malware scanning software.

Volume of Malware Successfully Propagated via Email Attachments



The volume of malware successfully propagated via email attachments declined slightly in 2008 versus 2007. These last two years represent a 40 percent drop-off relative to the previous two years, in terms of attachment-based attacks.

Mobile Phone Malware: Growing Profit Centers

2008 saw several instances of malware designed for and spread via mobile phones.

One example is SymbOS/Kiazha.A, a "ransomware" Trojan that runs on Symbian OS devices and deletes incoming and outgoing SMS (text) messages. When it infects a mobile phone, the phone will display a message asking the user to send money (to an undisclosed location, using a mobile phone recharge card) to have the device restored to normal function.

This Trojan is installed on the phone by SymbOS. Multidropper.A, which also installs SymbOS/Beselo, a worm that propagates by sending itself as MMS (multimedia) messages every two minutes to every contact in the mobile phone's phonebook. It can also propagate via Bluetooth, and copy itself to any memory card inserted into the phone, allowing it to recover from deletion. In another tactic to enhance propagation, SymbOS.Multidropper.A installs SymbOS/ComWar.C, which spreads via Bluetooth and replicates and monitors itself to ensure it is not erased from the phone.

During the last year, malware for mobile phones was largely circulated in Asia, where the number of people who own such devices is significantly higher than those who own personal computers. This makes spreading malware via mobile phones a potentially profitable endeavor for malware creators in that region.

The "Shadow" Internet Economy

Successful online criminals are making millions or hundreds of millions of dollars from their enterprises. These profits continue to drive innovation and specialization.

Like the legitimate Internet economy they shadow, the online criminal world has become a global, thriving network of product and service providers and consumers doing business together. In the short term, this specialization and collaboration are making online criminals more nimble and effective.

Those launching attacks are often no longer the developers creating the tools. Instead, attackers can select from an array of competing and increasingly sophisticated products and solutions. A wide range of well-designed malware offerings is currently for sale or rent, including:

- Botnet management and dashboard-type tools
- Mass blog posting tools
- Sophisticated volume spamming tools
- Automated webmail account creation tools (including some that defeat the CAPTCHA feature that webmail hosts such as Yahoo!, Gmail, and MSN use to prevent bots from opening webmail accounts)
- Account generators that enable spammers and scammers to bulk-post to Craigslist
- Keylogging programs

But in the longer term, the online crime economy may also be on its way to becoming a bureaucracy. The positive side to this: One unavoidable side effect of becoming more established is a paper trail, which may make it easier for law enforcement organizations worldwide to track and apprehend more of these offenders in the future.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Asprox: Transforming an Old Trojan

One of the most effective botnets of 2008 was Asprox, an old Trojan that was turned into a very sophisticated botnet and used in thousands of SQL injection attacks on legitimate websites. First used several years ago as a password-stealing Trojan, it was later upgraded to send phishing spam. Its big transformation occurred in May 2008, when Asprox started updating itself with a SQL injection tool.

This SQL injection tool looks legitimate to users of infected computers, running as "Microsoft Security Center Extension" (msscntr32.exe). Meanwhile, in the background, it is actually using Google to scan the Web for Active Server Pages (.asp), which can be susceptible to SQL exploits.

When the SQL injection tool finds vulnerable pages, it inserts a malicious iFrame into page content. The iFrame invisibly redirects a site visitor's browser to malsites that try various methods of infecting the victim's computer with malware and adding it to the Asprox botnet. To make it harder to detect to anti-malware programs, Asprox communicates via proxy server on TCP Ports 80 or 82.

Cisco data showed that at its peak, Asprox was successfully iFrame-injecting 31,000 different websites per day.

Botnet Trends

Botnets are the big "workhorses" that power many of today's online threats and criminal activities. Botnets consist of thousands of malware-compromised computers. Those who control the botnets can rent out the processing power and bandwidth available to these computers, or use it themselves.

Online criminals are using botnets for pretty much every aspect of Web-based threats, including spamming, sending DDoS attacks, infecting legitimate websites, hosting malicious websites (such as botsites), and propagating more malware.

The Storm botnet, enormously widespread in 2007, was only a harbinger of what was to come. New, even more sophisticated, robust, and scalable botnets, such as Mailer Reactor, Kraken, and an updated, powerful variant of Asprox (which had been around in a less able form for several years), have also had great success.

These botnets are designed as reusable platforms that can cycle, synchronize, and distribute dynamic attacks. Like many Web 2.0 technologies, they "promote" collaboration and depend on the network effect. They're adaptive and intelligent, and offer flexibility, redundancy, and security protocols inspired by modern peer-to-peer (P2P) networks.

The Importance of Social Engineering

Online criminals have developed an array of sophisticated social engineering techniques to entice victims to open an email or file, or to click on a link or online ad. The use and sophistication of social engineering techniques in online attacks continued to grow in 2008, and this trend is expected to continue during 2009 with even more—and better executed—attacks occurring via email, instant messaging (IM), and mobile devices.

One successful technique is creating spam campaigns based around "hot topic" news items and current events. Sometimes, these spam emails direct victims to a malicious site that will attempt to download malware to their computers.

But more sophisticated campaigns that include extremely clever phishing websites, and where both spam and websites use social engineering techniques tied to current events, have also become common.

With those campaigns, victims are lured to legitimate-looking websites where they are asked to provide personal information during what appears to be an actual transaction. However, victims do not receive the goods or services they thought they had purchased. Or, in cases where the fraudsters do send something, counterfeit or poor-quality items are delivered—for example, fake pharmaceuticals disguised as brand-name prescription medication.

The more effective email-attachment-based malware distribution campaigns of 2008 also used clever social engineering techniques.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

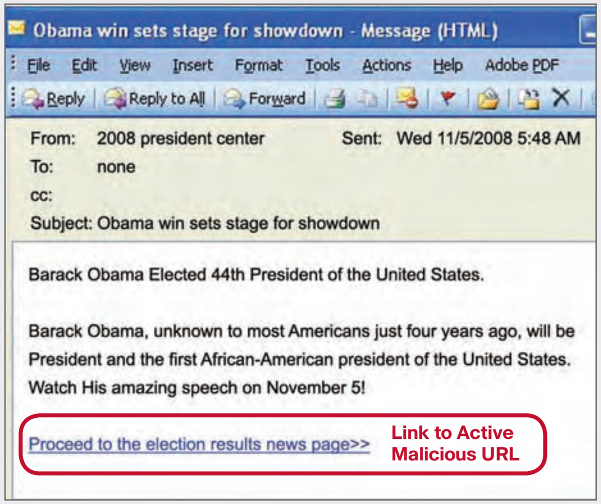
One type involved email claiming to be from UPS or FedEx, which asked the recipient to review an attached invoice or delivery confirmation to discover what happened to a fictitious package. When the victim opened the attachment, the malware installed itself and let the attacker gain control over the infected computer.

> “These virus-laden emails that claim they’re from FedEx or UPS are really clever. It’s no wonder people respond to them!”
>
> —Michael Postlethwait, Cisco Security Analyst

Another notable campaign occurred around U.S. tax-filing time. This one involved email that looked as if it had been sent by the Internal Revenue Service (IRS). It had a very official appearance, and played on the widespread fear of the IRS and worries about not opening or responding to its letters. Only the most savvy recipients realized that the IRS does not send notifications in email, but only uses paper mail sent via the U.S. Postal Service.

The continuing popularity of “scareware” can also be explained by viewing it as an example of successful social engineering techniques. Scareware pretends to be anti-malware or anti-spyware scanning software, but is actually malware that is taking advantage of computer users’ fear of spyware or malware to infect them. The websites these downloads are offered from often look extremely credible and professional, and often include fake logos and endorsements from industry organizations.

New President, New Malware



Obama win sets stage for showdown - Message (HTML)
File Edit View Insert Format Tools Actions Help Adobe PDF
Reply Reply to All Forward

From: 2008 president center Sent: Wed 11/5/2008 5:48 AM
To: none
cc:
Subject: Obama win sets stage for showdown

Barack Obama Elected 44th President of the United States.

Barack Obama, unknown to most Americans just four years ago, will be President and the first African-American president of the United States. Watch His amazing speech on November 5!

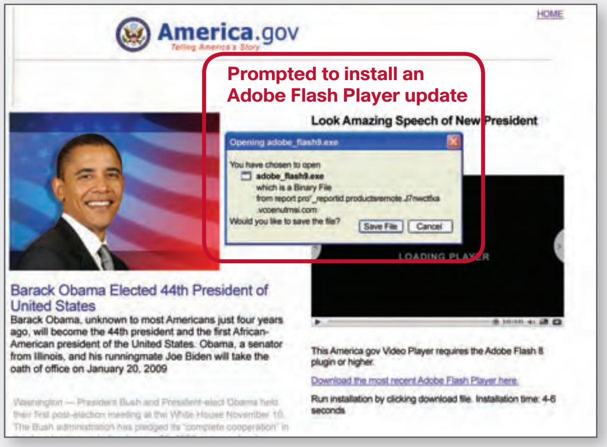
Proceed to the election results news page>>

Link to Active Malicious URL

Current events-oriented email messages convince recipients to open and act on the email. In a recent example, a spam campaign invited recipients to watch a video of President-elect Barack Obama’s victory speech. Subject line examples included:

- Election Results Winner
- The New President’s Cabinet?
- Obama Win Sets Stage for Showdown

The email directed recipients to a fake government-themed botsite. Once there, they were prompted to install an Adobe Flash Player update, which was actually data-stealing malware. Once installed, the malware stole screenshots and passwords, sending that information to a Web server located in Kiev, Ukraine.



Prompted to install an Adobe Flash Player update

Look Amazing Speech of New President

Opening adobe_flash9.exe

You have chosen to open adobe_flash9.exe which is a Binary File from report.pro'_reportid.productsremote.J7nwctfxa .vcoenufmsi.com Would you like to save the file?

Barack Obama Elected 44th President of United States

Barack Obama, unknown to most Americans just four years ago, will become the 44th president and the first African-American president of the United States. Obama, a senator from Illinois, and his runningmate Joe Biden will take the oath of office on January 20, 2009

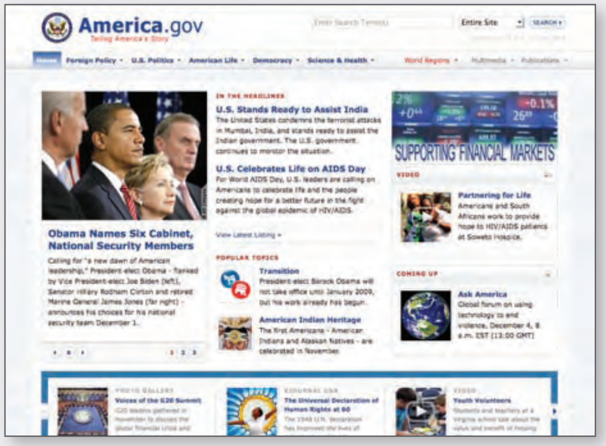
Washington — President Bush and President-elect Obama held their first post-election meeting at the White House November 10. The Bush administration has pledged its "complete cooperation" in

This America.gov Video Player requires the Adobe Flash 8 plugin or higher.

Download the most recent Adobe Flash Player here.

Run installation by clicking download file. Installation time: 4-6 seconds

Government-Themed Botsite



Obama Names Six Cabinet, National Security Members

Calling for "a new dawn of American leadership," President-elect Obama - flanked by Vice President-elect Joe Biden (left), Senator Hillary Rodham Clinton and retired Marine General James Jones (far right) - announces his choices for his national security team December 1.

U.S. Stands Ready to Assist India

The United States condemns the terrorist attacks in Mumbai, India, and stands ready to assist the Indian government. The U.S. government continues to monitor the situation.

U.S. Celebrates Life on AIDS Day

For World AIDS Day, U.S. leaders are calling on Americans to celebrate life and the people creating hope for a better future in the fight against the global epidemic of HIV/AIDS.

View Latest Listing

Transition

President-elect Barack Obama will not take office until January 2009, but his work already has begun.

American Indian Heritage

The first Americans - American Indians and Alaskan Natives - are celebrated in November.

Partnering for Life

Americans and South Africans work to provide hope to HIV/AIDS patients at Soweto Hospice.

Ask America

Global forum on using technology to end violence, December 4, 8 a.m. EST (13:00 GMT)

Voices of the G20 Summit

The Universal Declaration of Human Rights at 60

Youth Volunteers

The Real America.gov Site

In this example, recipients of a message—which claimed to include a link to Barack Obama’s victory speech—were actually directed to a botsite serving up data-stealing malware.

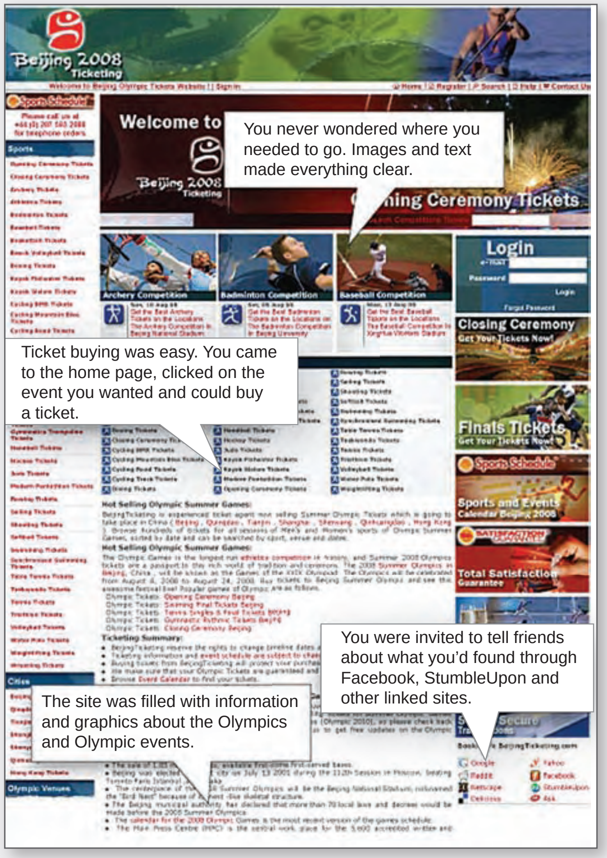
All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Beijing Olympics Fake Ticketing Scams

One of the most elaborate social engineering Internet scams of 2008 was related to the Beijing Olympics, with criminals making a profit of an estimated US$40 to $50 million. People in several countries, from New Zealand to the United States, were taken in by fake ticketing sites that sold illegitimate or nonexistent tickets to Olympic events. Some individuals paid thousands of dollars for particularly hard-to-come-by tickets, such as those for the opening ceremonies.

The biggest offender was Beijingticketing.com, a professional-looking website that featured the official Beijing Games logo. This fraudulent website was superior to the official ticketing site, with a better ticketing purchasing process and integration with social networking sites like Facebook to virally spread the fake site. Even MSNBC initially believed the site was credible: An MSNBC Forbes Traveler article featured a link to the site. This helped it gain a high search engine ranking, which resulted in ticket seekers who used search engines to look for tickets going to the fake site rather than legitimate sites.

Beijingticketing.com asked users to register—and provide confidential information—before they could purchase tickets. After registration, users provided credit card numbers and "bought" tickets, which they never received. Not only did the scammers net millions of dollars, but they also scooped up thousands of valid credit card numbers for later use or resale to other online criminals.



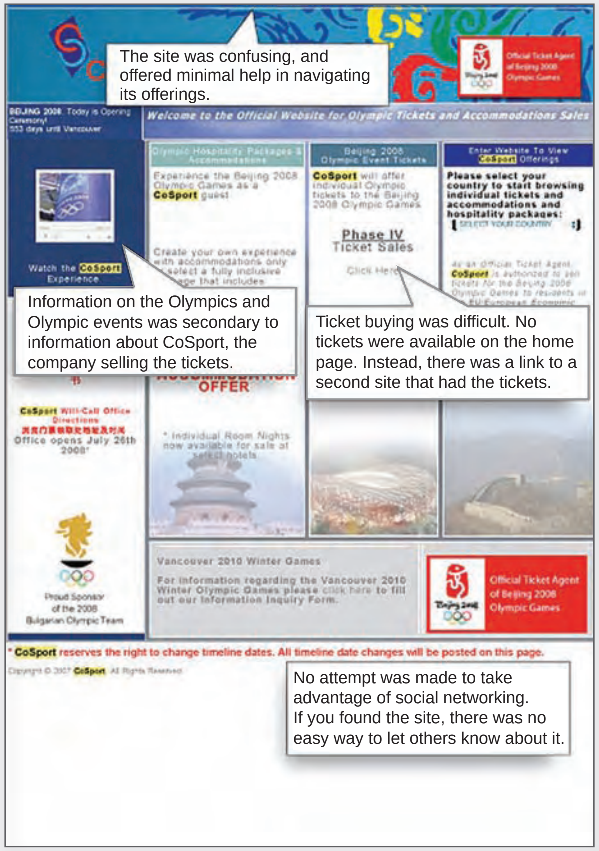
You never wondered where you needed to go. Images and text made everything clear.

Ticket buying was easy. You came to the home page, clicked on the event you wanted and could buy a ticket.

You were invited to tell friends about what you'd found through Facebook, StumbleUpon and other linked sites.

The site was filled with information and graphics about the Olympics and Olympic events.

Scam Ticketing Site


Welcome to the Official Website for Olympic Tickets and Accommodations Sales
Phase IV Ticket Sales
OFFER
Vancouver 2010 Winter Games
Official Ticket Agent of Beijing 2008 Olympic Games

The site was confusing, and offered minimal help in navigating its offerings.

Information on the Olympics and Olympic events was secondary to information about CoSport, the company selling the tickets.

Ticket buying was difficult. No tickets were available on the home page. Instead, there was a link to a second site that had the tickets.

No attempt was made to take advantage of social networking. If you found the site, there was no easy way to let others know about it.

Official Ticketing Site

Fraudulent Olympics ticketing websites, such as beijingticketing.com, took advantage of thousands eager to buy tickets to the 2008 Beijing Summer Olympics.

Source: www.beijingticketscam.com. Moriarty Leyendecker Erben LLP.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Spam and Phishing Trends

Cisco estimates that currently, more than 100 billion messages per day—or approximately 85 percent of all email sent worldwide—can be defined as spam. That's a significant increase in the volume from the previous year, and represents 100 spam messages per day for every Internet user on the planet. Spam has undergone a significant evolution in the last year. Massive volumes of pharmaceutical and get-rich-quick spam from botnets remain a resource- and processing-intensive issue for many organizations and service providers. Still, the network protection, anti-spam, and filtering solutions in place at most enterprises have made high-volume, low-sophistication spam more of an annoyance than a security issue.

The spam that does ultimately make it into recipients' inboxes is becoming ever more dangerous and attractive, and thus likely to be opened. Newer spam campaigns typically include "blended threat" spam messages, which incorporate URLs to entice recipients to click through to malware-distributing or phishing websites.

Another type of spam that has become noticeably more common this year involves targeted phishing, also known as "spear phishing." For these attacks, sophisticated online criminals have been using smaller phishing campaigns aimed at more targeted groups of recipients—to great effect.

Earlier phishing campaigns were widespread and high-volume, and typically pretended to be from large banks with a national presence. Then, an increasing number of phishing campaigns started using the identities of regional and local banks located near the recipient (and thus involved fewer messages per campaign).

The latest types of spear-phishing campaigns include:

- Spam sent via SMS to the mobile phones of recipients in the same area code
- Email pretending to be from universities with which the intended victims are affiliated as current students, alumni, or faculty
- Email that attempts to lure the victim into entering login information about their Google Adwords account (not only is the victim's credit card or personal information stolen, but often, their Adwords traffic gets redirected to criminal-run blogs)
- "Whaling" emails, which are extremely personalized to target specific top executives

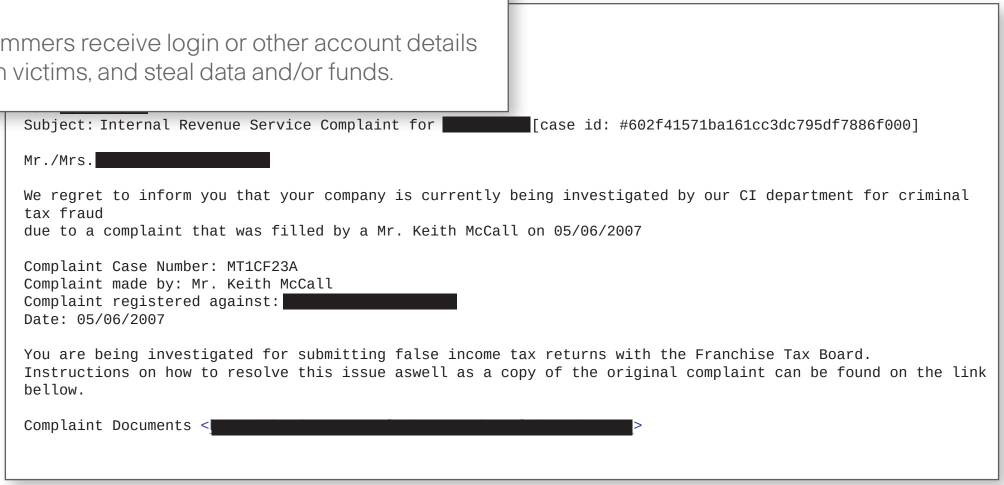
Spear-Phishing Examples

Spear-phishing messages currently represent about one percent of all phishing campaigns, but are expected to become more prevalent. This trend bears close monitoring, because the attacks are becoming more sophisticated: Criminals are investing time and resources in personalizing spam and making the messages seem credible. Why? Because the jackpots are higher when they succeed in obtaining sensitive personal data from specially targeted, attractive victims.

Typical spear-phishing attacks consist of four steps:

1. By launching malware, hacking into networks or buying lists from other nefarious online resources, scammers obtain a specialized distribution list of valid email addresses.
2. They register a domain and build a fake (but credible-looking) website to which phishing email recipients are directed.
3. They send phishing emails to their distribution list.
4. Scammers receive login or other account details from victims, and steal data and/or funds.

Spear-phishing attacks require criminals to efficiently build appropriate resources and trick victims into revealing valuable private information.



```
Subject: Internal Revenue Service Complaint for [redacted][case id: #602f41571ba161cc3dc795df7886f000]

Mr./Mrs.[redacted]

We regret to inform you that your company is currently being investigated by our CI department for criminal
tax fraud
due to a complaint that was filled by a Mr. Keith McCall on 05/06/2007

Complaint Case Number: MT1CF23A
Complaint made by: Mr. Keith McCall
Complaint registered against:[redacted]
Date: 05/06/2007

You are being investigated for submitting false income tax returns with the Franchise Tax Board.
Instructions on how to resolve this issue aswell as a copy of the original complaint can be found on the link
bellow.

Complaint Documents <[redacted]>
```

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Spear-phishing emails often succeed because they mimic messages from an authoritative source, such as a financial institution, a communications company, or some other easily recognizable entity with a reputable brand.

Unlike more common “mass” phishing emails, however, spear-phishing attacks rely on specific (usually stolen) information to craft a more personalized message—one the recipient is more likely to open and respond to. The personalized approach of spear phishing, combined with email reputation hijacking, in which criminals use a legitimate email provider’s infrastructure to send messages, makes it more difficult to weed out these emails via standard anti-phishing technologies.

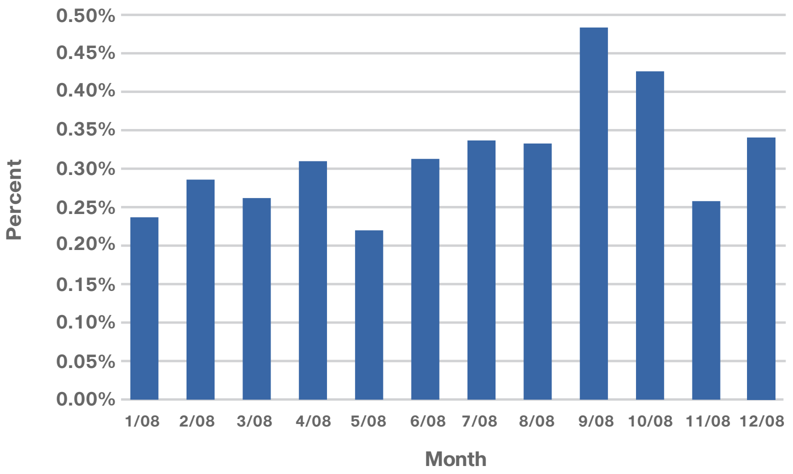
In many cases, online criminals rent or steal lists of valid email addresses, and can therefore personalize outgoing messages. Consequently, even savvy Internet users—conditioned to ignoring the less-sophisticated phishing messages sprayed to millions of people at the same time—can be lured into handing over login names, passwords, and other sensitive information.

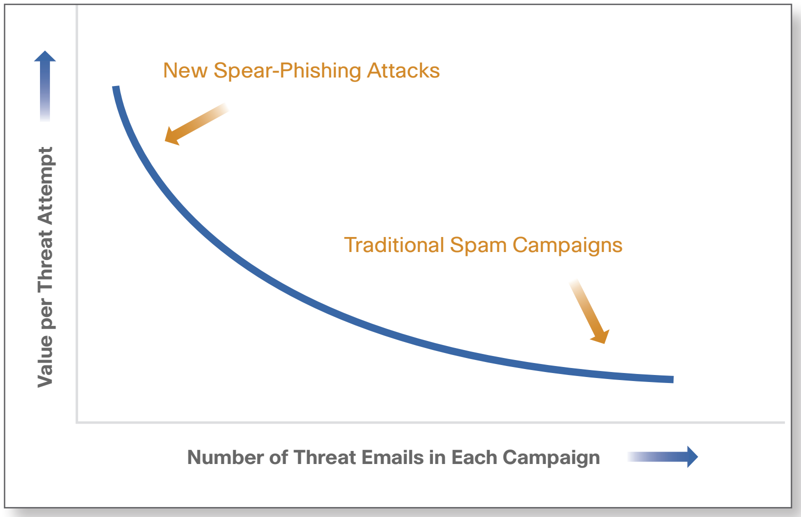
For example, online criminals have been sending spear-phishing messages that appear to be from entities such as:

- The Internal Revenue Service, explaining that the recipient or the company is being audited.
- The Better Business Bureau, which has received a “complaint” about the recipient’s company.
- U.S. district courts or tax courts, notifying recipients that they are being subpoenaed.

These messages look authentic and typically ask recipients to rapidly respond to the inquiry, which usually includes an attached “explanatory document.” However, when opened, this file actually launches malware in the background to take control of the recipient’s computer or network, or to install a keylogging program.

Targeted Attacks as a Percentage of Spam




New Spear-Phishing Attacks
Traditional Spam Campaigns
Value per Threat Attempt
Number of Threat Emails in Each Campaign

Spear-phishing campaigns are sent to fewer recipients, but are more likely to offer higher returns to criminals when recipients do respond to them.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Email Reputation Hijacking

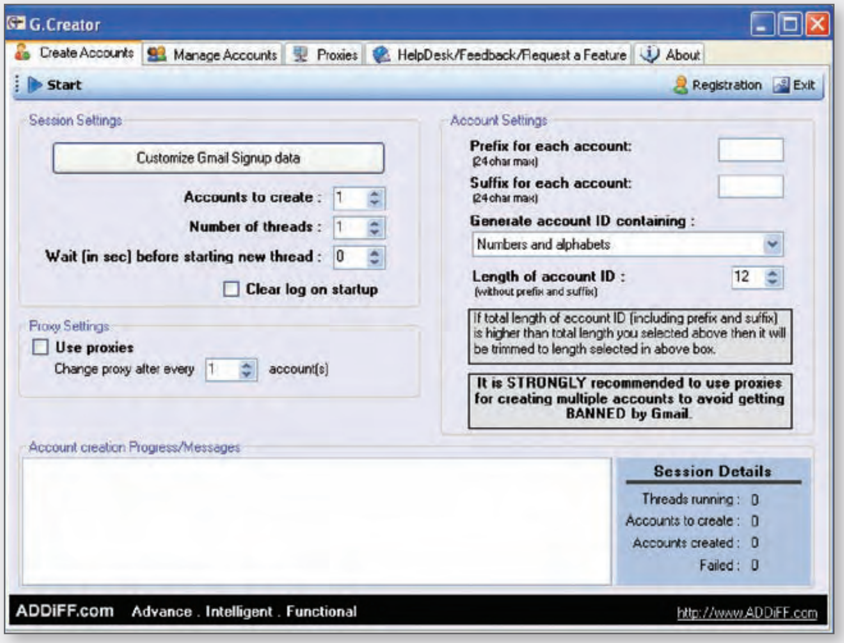
In email reputation hijacking, real email accounts with major legitimate webmail providers are used to send out spam. Taking advantage of the webmail provider's positive reputation offers increased deliverability: It makes the spam harder to detect and block, since it has the webmail provider's headers and formatting, and anti-spam solutions cannot block the mail servers of large webmail providers like Yahoo!, Gmail, and Hotmail.

The appeal of reputation hijacking has led to growth in the number of commercial tools available to spammers. These tools are aimed at making it simpler for spammers to create accounts, defeat CAPTCHAs, post, and rotate IP addresses to target webmail providers like Gmail, Yahoo!, and Hotmail, as well as sites like MySpace, Craigslist, and blogs.

Cisco estimates that during 2008, spam due to email reputation hijacking from the top three webmail providers—Microsoft, Gmail, and Yahoo!—accounted for just under one percent of all spam worldwide, but constituted 7.5 percent of all these providers' mail. The average spam rate from each webmail provider rose significantly for a period of time after tools to take advantage of their systems became available.

For example, in January 2008, Russian hacker "John Wane" defeated Yahoo!'s CAPTCHA. This led to an HTTP spike, followed by a three-month SMTP blitz. In May 2008, Google's CAPTCHA was broken, which led to an enormous spike in account creations. In August 2008, "John Wane" released AOL CAPTCHA-breaking code.

Email Reputation Hijacking Tools


G.Creator
Create Accounts
Manage Accounts
Proxies
HelpDesk/Feedback/Request a Feature
About
Start
Registration
Exit
Customize Gmail Signup data
ADDiFF.com Advance . Intelligent . Functional
http://www.ADDiFF.com

Session Settings

Accounts to create : 1

Number of threads : 1

Wait (in sec) before starting new thread : 0

□ Clear log on startup

Proxy Settings

□ Use proxies

Change proxy after every 1 account(s)

Account Settings

Prefix for each account: (24char max)

Suffix for each account: (24char max)

Generate account ID containing : Numbers and alphabets

Length of account ID : (without prefix and suffix) 12

If total length of account ID (including prefix and suffix) is higher than total length you selected above then it will be trimmed to length selected in above box.

It is STRONGLY recommended to use proxies for creating multiple accounts to avoid getting BANNED by Gmail.

Account creation Progress/Messages

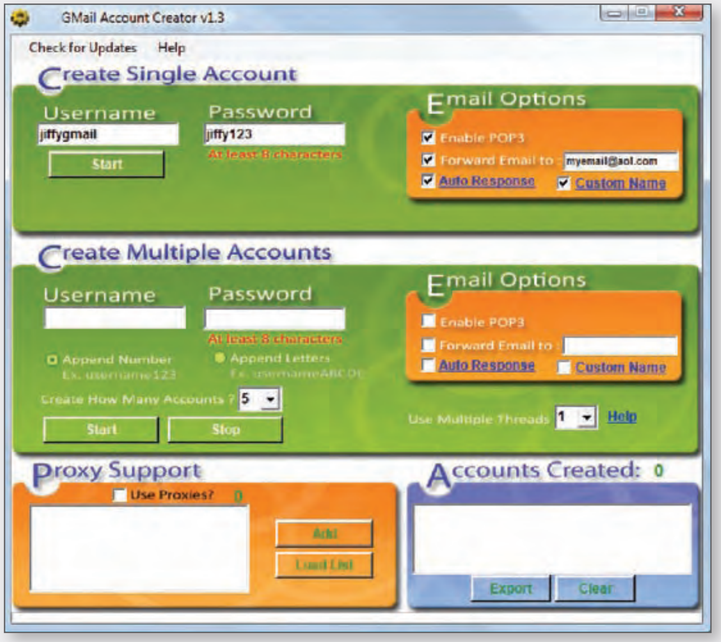
Session Details

Threads running : 0

Accounts to create : 0

Accounts created : 0

Failed : 0



Create Single Account

Username: jiffygmail

Password: jiffy123

At least 8 characters

Email Options

☑ Enable POP3

☑ Forward Email to : myemail@aol.com

☑ Auto Response ☑ Custom Name

Create Multiple Accounts

Username

Password

At least 8 characters

○ Append Number Ex. username123

● Append Letters Ex. usernameABCDE

Create How Many Accounts ? 5

Email Options

□ Enable POP3

□ Forward Email to :

□ Auto Response □ Custom Name

Use Multiple Threads 1

Proxy Support

□ Use Proxies? 0

Accounts Created: 0

Email reputation hijacking tools for the major webmail providers are commercially available and easily obtained. These tools were used frequently in 2008 and spam originating from these webmail providers increased significantly.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Data Loss

Despite best efforts, security incidents related to data loss are on the rise. Data loss can occur because of the physical loss or theft of systems and storage devices or the accidental sharing of information in an insecure fashion. Online criminals are using malware to steal consumer and company data online. Hackers are also getting their hands on data by breaking into insecure or weak systems and devices. And sometimes, insiders are the culprits.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

More and more businesses are recognizing that their data is a precious asset that must be protected. PricewaterhouseCoopers' *2008 Global State of Information Security Study* reports that many more organizations are encrypting "sensitive information not just in laptops, but also in databases, file shares, backup tapes, and removable media." And many have made "significant strides in advancing Web/Internet capabilities," including content filters, website certification/accreditation, and secure browsers. The report also cites increased use of technologies that help protect wireless devices, and tools that can discover unauthorized devices or prevent intrusions.

According to the Privacy Rights Clearinghouse's *Chronology of Data Breaches*, since January 2005, more than 230 million records have been compromised due to security breaches. Cisco research shows that inadequate data security can have significant consequences for organizations, including business disruption, reduced productivity, and increased operational expenses—and those are on top of the obvious loss of sensitive data.

Data loss related to the loss or theft of equipment is an enormous problem for businesses and individual users. Ponemon Institute recently reported that the number of lost laptops at some medium-sized and large airports has been reaching more than 600,000 annually. More than half of the laptops are never reclaimed, as many people hold no hope their laptop will be found. Therefore, they often do not bother taking any steps to attempt to locate and retrieve them.

The following incidents that occurred in 2008 are related *just* to laptops:

- A laptop computer containing personal information—including names, addresses, and employee identification numbers—for approximately 13,000 workers of a global pharmaceutical company was stolen from an employee's car. The laptop was encrypted, but the flash drive was not; the latter contained potentially sensitive business information, according to a company spokesperson.
- In the summer of 2008, Verified Identity Pass (VIP), a vendor of the U.S. Transportation Security Administration that operates a Registered Traveler program under the brand Clear, temporarily misplaced a laptop that had been reportedly locked in an office at San Francisco International Airport. The laptop contained unencrypted personal information for 33,000 customers, but according to the vendor, none of the data was compromised.
- The U.S. Veterans Affairs (VA) Department, which suffered severe embarrassment in 2006 when a laptop containing millions of veterans' records was stolen, had its new security policies put to the test in spring 2008, when another of its laptops was stolen from an employee's Texas apartment. This time, the data was encrypted, no one without proper authentication could access the computer, and the VA knew which piece of equipment was missing. The employee also did his part by immediately reporting the theft to the VA and local authorities.
- The U.K.'s Ministry of Defense reported a serious breach of security when a laptop containing unencrypted data related to 600,000 prospective military recruits, including some financial and passport information and medical details, was stolen from a military recruitment officer's car.

Fortunately, very few incidents of equipment loss or theft result in information being passed on to criminals with the expertise to profit from accessing and using the compromised data. These are usually simple thefts, with the end goal of quickly reselling the equipment, which is wiped clean of data to conceal the fact it has been stolen.

Data Loss Issues on the Regulatory Radar

Data breach notification legislation now requires that companies report when sensitive data is potentially lost—such as when a laptop is stolen.

Currently, 42 U.S. states and the District of Columbia have data breach notification laws on the books, or legislation pending approval. While state laws vary, they generally follow the California Security Breach Information Act (SB-1386), which requires organizations that electronically store personal data about customers to inform those individuals if the company knows the security of that information has been compromised.

Meanwhile, the U.S. government is attempting to address these notifications at the federal level and consolidate the variances in state laws—perhaps even strengthening some laws. It is also trying to align federal legislation with approved or pending legislation in other countries.

In addition, there are increasing laws and regulations to handle the sharing of sensitive data. New U.S. compliance regulations and market-driven industry best practices were released in 2008 that attempt to focus on stronger protection and increased enforcement for data loss violations. The federal government released the Red Flags provision of the new Fair and Accurate Credit Transactions Act, which spans multiple industries and requires businesses that provide services before billing to implement an identity theft prevention program. The initial enforcement period was November 2008, but it has been delayed to May 1, 2009.

In October 2008, the state of California passed two privacy laws, SB-541 and AB-211, that attempt to augment existing medical privacy compliance regulations by focusing on the enforcement of unauthorized access to patient health information, negligent disclosure of patient records, and illegal use of medical information for financial gain. The Health Information Trust Alliance will also release the HITRUST Common Security Framework (a market-driven

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

best practice) in January 2009. This framework is built upon industry standards such as ISO 2700x, B/S 7799, PCI, and the NIST 800 series.

Individual U.S. states are also imposing their own laws to mandate encryption of personal information sent over the Internet by businesses located in the state. New laws and regulations require, among other things, encryption of personal information on laptops, PDAs, and portable media (including flash drives); encryption of personal information transmitted over the Internet; development and publication of Social Security number (SSN) privacy protection policies; and specific measures to protect the confidentiality and security of employee SSNs.

While such legislation obviously benefits those whose data has been compromised, disclosing a security breach may leave an organization subject to negative media coverage and possibly cause long-term reputation damage. This can lead to a drop in the confidence of users and customers, who may be inclined to take their business elsewhere.

Many laws and regulations carry significant statutory penalties for violations as well as the possibility of businesses facing private rights of action for noncompliance. As a result, an increasing number of businesses are using encryption and other access control technologies to help ensure compliance.

The Limitations of Compliance

While many regulatory standards attempt to help protect user data, compliance cannot be a security placebo. Many companies have made great strides to achieve compliance measures, but the sense of urgency that often surrounds compliance demands should not become a distraction from other, crucial threats to security. By focusing almost exclusively on compliance and aligning procedures to meet those requirements, organizations can lose sight of the rapidly evolving risk and threat environment. In fact, multiple security incidents in 2008 involved organizations that were considered "compliant," but were compromised by exploits not covered by compliance requirements. Many compliance procedures do not and cannot address today's array of applications, technologies, tools, and the related security vulnerabilities that are increasingly being targeted by threats. Instead, compliance measures are intended to help organizations achieve specific objectives that mitigate only *certain* security risks.

The market-driven Payment Card Industry Data Security Standard (PCI DSS), for example, focuses on the protection of cardholder data during processing, transmission, or storage. It is a detailed standard compared to other compliance regulations. However, it does not entirely mandate a strong level of security, as it must balance its strict requirements with a risk-based approach that can apply to both small and large organizations. The industry recently updated PCI DSS to version 1.2. In addition to merging both versions of the requirements and testing validation steps, the revised standard provides new deadlines around Wired Equivalent Privacy (WEP) replacement and adopts a risk-based analysis approach so to help smaller businesses comply.

To address the array of compliance best practices and regulations, organizations will likely plan larger IT governance, risk management, and compliance (GRC) programs. Although achieving compliance is important, organizations must remember that many best practices and regulations apply only to protecting certain information—for example, company financial information (Sarbanes-Oxley), patient medical information (HIPAA), and personally identifiable information (Basel II, and U.K. and EU data laws). Therefore, in addition to regular compliance reviews, organizations will often conduct top-down gap analyses to improve existing procedures and proactively meet current and emerging threats.

Recycling Risks

Recycling of electronics equipment is becoming more common. In fact, some countries already charge buyers a recycling fee when they purchase any electronics item. All or part of that fee may be reimbursed if, at the end of its useful life, the item is taken or sent to a recycling center. Organizations—looking to recoup those fees, comply with laws and regulations, or simply be more environmentally responsible—are likely to recycle more often. Yet while more organizations are recycling their "e-waste," many aren't taking sufficient precautions to make sure those items have been wiped clean of sensitive data.

Once equipment destined for recycling is sent away, there is no telling where it may go or what will happen to any data that can be extracted from it. Press reports indicate that some devices have ended up as far afield as Indonesia and West Africa, where salvaged data is sold at bargain-basement prices.

Many organizations do not make the IT department responsible for (or at least involved in) the electronics equipment recycling process, instead leaving it to other departments, such as facilities management. However, it is unlikely that personnel outside of IT will be aware of the importance of degaussing hard drives and otherwise safeguarding potentially sensitive data on defunct devices before those devices end up in a recycling facility. Consequently, organizations without clear, security-oriented policies for how to and who should handle this process within the organization may put sensitive data at risk.

Identity Theft

Identity theft continued to rise during 2008 and shows no signs of slowing down. Many online criminals have been successful at using social engineering tactics that feed on the trust of others, and allow sensitive personal data to be harvested, ranging from Social Security and driver's license numbers to complete medical histories.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Collating data from a variety of publicly available sources—including user profiles on popular social and professional networking sites—makes it easy to pull together enough information about a person's identity to create a scheme that either takes advantage of the individual, or of people who they know and who trust them.

For victims of identity theft, the risks have increased significantly: Just one security breach—whether it is keylogger malware invisibly downloaded to their home computer by a compromised website, or hackers cracking into the customer database of their favorite retailer thousands of miles away—can compromise their personal information.

And now, stolen personal information is being bundled and sold to criminal elements around the world—such as organized crime rings or even hostile governments. Those who tap this market use the information not only for profit, but also to sell to those who use the information for terrorism-related activities, such as creating fake passports and other travel documents, or laundering money for terrorist cells.

Targeting the Masses

Although the instances of highly targeted phishing campaigns are growing in number, most online criminals looking to commit identity theft are not going out of their way to target specific individuals or groups—at least, not yet. They are simply trying to snare as many people as possible.

The Internet provides ample opportunities for identity thieves looking to target the masses. According to a report released by the U.S. Federal Trade Commission (FTC) in February 2008, some 64 percent of fraud complaints in 2007 related to incidents where the method of initial contact was an Internet solicitation, such as email.

The economic impact to individuals who are victims of identity theft is obvious. But businesses also suffer in terms of reputation damage and financial loss, particularly in instances when the trust of many consumers has been compromised. For example, sophisticated phishing techniques can dupe users into believing they are interacting with a trusted source—such as an individual, charity organization, bank, or online retailer—via spam emails and with legitimate-looking but fake websites.

Other data-gathering opportunities for today's identity thieves include:

- **Social networking**—A rich trove of personal information, including phone numbers, addresses, full names, and birthdates, is available on user profiles posted on social networking sites such as Facebook and MySpace, and additional personal information such as mothers' maiden names on sites like Ancestry.com.
- **File sharing and peer-to-peer software**—When users allow friends and associates to access certain files, such as MP3s, other files on their computers can be easily compromised. "Access creep" is also a growing problem in collaborative work environments, with people being allowed to view too much information, including company secrets and information about coworkers.
- **RFID tags**—Some concealable readers can read radio frequency identification (RFID) tags from a short distance (up to a few feet) to gather data from credit and other types of cards. RFID tags can be cloned, and the equipment required to do this is available. This has clear security threat implications: RFID technology is used in everything from building access cards to passports.

Rethinking Identity Management

Given the concerns around data loss and identity theft, the recent resurgence of interest in identity management is not surprising. Many leading companies are overhauling the security platforms they have long relied on and adopting new identity management technology. They look to prevent data loss, reduce the potential for identity theft, limit opportunities for insiders to engage in criminal activities, and comply with regulatory standards. They also require technology that supports collaboration among their remote workforce using Web 2.0 tools and applications, as well as with other organizations.

Today's identity management solutions have advanced well beyond easy-to-compromise usernames and passwords required to access networks or applications. Secure, personalized user profiles may be created. And before access is approved, users may have to be verified through one or more methods, including tokens or smart cards. Some organizations use biometrics, including fingerprints and iris scans, to authenticate users.

Transparency is another theme in modern identity management. Organizations want technology that allows them to monitor user activities from sign-on to sign-off. They need solutions designed to set boundaries on the amount and types of information and other resources users are permitted to access. In addition to making it easier to track user activity, identity management technologies now on the market allow organizations to set consistent user policies and conduct auditing and reporting to help assure compliance with regulatory standards.

There is strong demand for identity management solutions that are complete and highly effective but also easy to use. That's why more organizations are looking to "single sign-on" solutions that simplify the process of verifying user identity and give users access to the information and applications they need. But while identity management technology has advanced dramatically in recent years, the industry continues working on developing solutions that provide even greater security and user monitoring capabilities—and don't hinder workforce productivity.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

The Human Factor

People are still the weakest link in the security chain. But their capacity to learn and modify their behavior in response to information means they also represent an area with a great opportunity for improvement. Attacks on websites and corporate networks continue to increase in sophistication, and online criminals are growing proficient at duping even the savviest or most cautious of users.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Human Nature Invites Risk

Plain and simple human error—such as a CEO opening an email that appears to be from a trusted source, but is really a well-disguised "whaling" attack, or poor judgment, such as engaging in e-commerce on a website that does not have a valid security certificate and is a front for a scam—is often what triggers the release of malicious attacks or leads to identity theft and other fraud.

Human carelessness—for example, losing an employer-issued laptop or inadvertently posting a company's sensitive information on a blog—can also quickly turn into a reputation-damaging event, and cause significant financial loss for an organization. Email address errors are another common human mistake-based security problem that can easily result in highly sensitive information being sent to the wrong people.

Even the security-conscious U.S. military is not immune to such blunders: In 2008, it was reported that United States Air Force (USAF) personnel inadvertently sent email messages intended for USAF personnel stationed at Royal Air Force Base RAF Mildenhall in Suffolk, England, to a tourist website with a similar email address. The maintainer of that site, which is intended to promote tourism in Mildenhall, notified the USAF several times about the emails but was told not to be concerned. Only when officials were notified that flight plans for a presidential visit were received did they become—reactively—alarmed.

Technology solutions (such as anti-spam tools and outgoing email monitoring) can be helpful for proactively mitigating some risks and preventing widespread damage from certain types of attacks. Providing ongoing threat education and training for employees—and building their awareness about security risks and the importance of safeguarding data—remain important security defense measures for organizations. But they have their limitations. Technology can create a false sense of safety, and neither that or education can address a broader security problem: human nature.

By nature, most people are curious, eager to communicate, and interested in good deals or attractive "freebies." Quite often, they also are overconfident that *they* are not the type of people who would fall prey to trickery or scams; this aspect of human behavior is a key element in making online crime work.

Online criminals thrive by taking advantage of Internet users' trust and human nature. Countless people continue to be lured to malware-distributing or phishing websites by emails containing URLs. Given that more than 80 percent of spam messages now contain URLs, it is not difficult to see why this hit-or-miss approach succeeds. And with potent and self-propagating malware available, even a relatively small number of infected users can infect many more.

Remote Working, Social Networking: Opportunities and Risks

Having a mobile workforce can significantly improve business productivity, and keep workers happy by allowing for better life-work balance. A global workforce can be very cost-effective, allowing for localized service to customers in different regions and faster entry into new markets. And many workers today (especially young, highly wired "Generation Y" workers) love using new tools and technologies that make work and life easier and more fun.

Organizations are equipping their remote workforces with the collaborative tools and mobile devices they need to do business anywhere, anytime. But by doing so, they also create security risks. For example, in its *Emerging Cyber Threats Report for 2009*, Georgia Tech Information Security Center warns that as Internet telephony and mobile computing—which are essential to remote workers—handle more and more data, they will become more frequent targets of online crime. The report predicts that criminals will be "drawn to the VoIP medium to engage in voice fraud, data theft, and other scams—similar to the problems email has experienced."

Meanwhile, the line between technology use for personal and professional purposes is becoming increasingly blurred. Recent Cisco research revealed that 44 percent of employees share work devices with others without supervision, and 46 percent said they transferred files between work and personal computers when working at home.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

A report by Telework Exchange and Sprint Nextel on wireless Internet usage among U.S. government employees revealed that 33 percent of teleworkers, and 11 percent of IT workers, were not familiar with security guidelines for using wireless Internet.

Cisco's recent research into security perceptions and online behavior of remote workers in several countries (including Brazil, France, India, and the United States) showed that using work computers and devices for personal use is a widely accepted practice today. A primary reason for this casual attitude cited by survey respondents: The belief that their employer does not mind. What's more, many users download certain tools and applications in an effort to be more efficient in their jobs, but can wind up derailing overall productivity by unknowingly creating a convenient inroad for a threat.

Elements of human nature, such as being curious and having the desire to connect with others, also create risk for organizations, which can expect more of their employees (mobile or otherwise) to engage in social and professional networking online while on the job. Some companies are encouraging this activity—using such outlets for their own marketing, PR, and HR initiatives. Even the microblogging utility Twitter is now being used by leading companies to share product news and offer special deals to those who sign up for the service.

Providing proactive and thorough user education, and setting clear policies about social networking and other online activities while at work, is good practice. However, many organizations either fail to set appropriate use policies or do not communicate them to users or internal resources expected to help enforce such practices. A report by Telework Exchange and Sprint Nextel on wireless Internet usage among U.S. government employees revealed that 33 percent of teleworkers, and 11 percent of IT workers, were not familiar with security guidelines for using wireless Internet.

Inadequate or insufficiently communicated appropriate use policies will have to change. With popular sites such as MySpace and Facebook likely to remain highly vulnerable to hard-to-detect malware such as Koobface, organizations will need to pay more attention to on-the-job social networking by employees. Koobface works to turns infected users' computers into botnet nodes. The worm searches for cookies associated with a social networking site and, once located, modifies them and embeds malicious links on a user's profile. Others viewing the profile assume the links were put there by the user. Trusting the source, they click on the links and also become infected with malware. (Instructing workers to clear their cookies on a daily basis can help combat this problem.)

Meanwhile, the laptops, mobile phones, PDAs, and data storage devices that both remote and onsite workers are using to engage in business and personal activities are providing myriad points of entry for spam, viruses, and malware. They also offer endless opportunities for loss of intellectual property and other data.

Workers may be insufficiently aware of the unprotected nature of mobile phones, the need to use privacy screens while doing sensitive work in public places, and taking extra care with easily misplaced mobile devices. A thumb drive can now contain as much as 64 GB of data, and the U.K. Ministry of Defense recently had to admit to several instances of sensitive information lost by officials moving data physically between locations, including a classified report on Al Qaeda, which was left on a train.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Using Social Networking and Web 2.0 Sites for Online and Offline Crime

Social networking websites such as Facebook, MySpace, Bebo, LinkedIn, Orkut (extremely popular in Brazil), and vKontakte (in Russia) have all been linked to spam and malware attacks. The Web 2.0 widgets and different types of potentially vulnerable content that users can add to their pages may make it especially easy for malware creators to exploit these websites in the year ahead.

Yet not all criminal uses of social networking and Web 2.0 sites take place exclusively online. Canadian and U.S. anti-fraud organizations reported a disturbing trend that surfaced in 2008: A sharp uptick in phone calls used in extortion schemes targeting senior citizens, which have resulted in victims paying thousands of dollars to criminals. The caller relays a fictional story about the senior's teenage or college-age grandchild needing to make bail in Canada—likely gathering personal information to use in the scam, such as the names of victims' grandchildren, from profiles posted on social networking and other Web 2.0 sites.

It also works the other way around, with online criminals "borrowing" elements from the physical world to help make their online scams appear credible.

Online scammers have been running so-called "419" (named after the section of the Nigerian penal code, where such scams often originate) or advance-fee fraud—a confidence trick that has been around for decades—on websites such as LinkedIn and Craigslist. A typical Craigslist scheme: The criminals use legitimate but outdated house-for-rent postings from other Craigslist users to dupe potential renters into wiring money to the "landlord," who claims he or she had to suddenly move overseas, and must rent out his or her house immediately—and cheaply.

In some cases where an address for the home is provided in the ad, victims have been told by the scammer that while a property tour was not available, they should drive by the house to have a look. While there may be plenty of red flags visible in retrospect, for many people seeing is believing, which is why this scam has been successful.

In another recent social engineering scheme involving Craigslist, a resourceful bank robber enlisted "help" for a robbery getaway through false advertising. The suspect posted a listing on the site advertising a road maintenance project that would pay US$28.50 per hour. Around a dozen unsuspecting decoys-to-be who applied were asked to show up for work at a local bank wearing specific attire—a yellow vest, safety goggles, a respirator mask and, if possible, a blue shirt.

They did as instructed, but when they arrived at the jobsite they found no work to be done and no contractor. At the same time, the robber (wearing the same gear as the decoys) wrestled a bag of cash from an armored truck guard and made a clean getaway—leaving the police to sort through a dozen look-alike suspects.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Insider Threats

External threats such as Web-based malware and hacker intrusions may be more numerous, but organizations should never ignore the significant security risks posed by insiders. Insider threats can be even more damaging to a company's reputation and financial well-being than ones that originate outside the organization.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Adding to concerns about insider threats, larger entities such as competing corporations and hostile governments (as well as organized crime) have been placing agents within organizations they wish to compromise. The extreme volatility and deep uncertainty felt throughout the global economy in the latter half of 2008—which will likely carry well into 2009—is another reason why insider threats can be expected to remain a major security concern for businesses of all types.

This year saw a rise worldwide in the number of instances of fraud, hacking, and identity theft by insiders—or those who were able to compromise physical security controls to gain access to an organization's networks. Underscoring this trend are the following incidents reported in the past year that were not discovered until after significant financial damage had occurred:

- In January 2008, a trader for French bank Société Générale admitted that by engaging in unauthorized stock market deals, he had caused a €4.9 billion loss for the financial institution. The employee used knowledge and experience he'd gained through previous work in the bank's risk management office to conceal his losses through falsified transactions.

  The trader's fraudulent activity—which required a breach of five layers of control and included the theft of computer access codes—was discovered by auditors looking into an error made by the bank's chairman and CEO. It is believed this trader acted alone, and was motivated not only by the desire for personal gain, but to enhance his trading reputation within the organization.

- In May 2008, three men (with direct access to the hardware targeted in the crime) were charged with hacking into 11 cash register terminals and stealing credit and debit card numbers from customers at a popular U.S. restaurant chain. A "packet sniffer"—a computer code designed to capture communication between computer systems on a single network—was installed on point-of-sale servers at the targeted restaurants. Over the course of seven months in 2007, data was collected from thousands of credit and debit cards. At just one location, more than 5000 cards were compromised, resulting in at least US$600,000 in losses for the financial institutions which issued the cards.

- There was even more bad news for the U.S. mortgage industry in 2008 when an investigation of mortgage brokers in the state of Florida, conducted by *The Miami Herald*, revealed that thousands of licensed brokers had criminal records that should have been discovered during mandatory background checks. Regulators must approve licenses for mortgage brokers in Florida, where background checks have been required since 2006. According to the newspaper's report, more than 10,500 people with criminal records were approved to work in the mortgage profession.

  The investigation uncovered an estimated US$85 million in losses due to fraud, identity theft, and theft of savings and homes involving licensed brokers. In addition, several brokers who committed fraud were—remarkably—allowed by regulators to keep their license. With public records and the current technologies available to anyone with an Internet connection, conducting background checks is a relatively simple, inexpensive, and quick control that can identify potential security issues.

- In October 2008, an onsite IT contractor for Shell Oil was caught stealing information about current and former U.S.-based employees from a company database. According to Shell, the contractor used Social Security numbers belonging to four employees to file fraudulent unemployment claims. After discovering the breach, Shell had the contractor removed from the premises. The company dropped its contract with the associated vendor and alerted its employees of the breach. The Texas Workforce Commission and local law enforcement are investigating the incident.

Financial Crisis May Heighten Insider Risk

Due to the global financial downturn, Gartner analysts are predicting large IT budget cuts as well as hiring freezes and layoffs. If workforces are to be cut in response to the financial pinch being felt by many organizations, many employees could become disgruntled "about-to-be-ex-employees." And these individuals could offer many opportunities for online criminals to gain access to sensitive data, passwords, and IT infrastructure.

For instance, consider the World Bank. According to some reports, an IT consultant infected the computers of several coworkers with keylogging software, gaining the ability to compromise several of its servers. As of mid-October 2008, the World Bank denies that sensitive information was compromised, but this story showcases the vulnerability of institutions and organizations that were otherwise perceived as robust and trustworthy.

With many companies globalizing their workforces, we are increasingly living in a single, integrated world economy. Employees of American banks and IT firms may be working out of call centers in Asia or Europe. Making sure the security policies put in place are usable in the context of local culture, but also work within the global security policies of a multinational organization, is crucial. In addition, as companies cut costs they may increase their dependence on teleworkers and consultants. This can be cost-effective, but requires additional security policies and implementations to work securely at the edges of an organization's network.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Issues of Trust

Many users believe they enjoy the same levels of data security they enjoyed in the past, when transactions and related data existed primarily in the physical realm. They trust that organizations they willingly give their personal information to will do everything possible to safeguard it. And they believe the equipment and services of providers they know and trust are secure.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Users can put their information at risk of exposure in more ways than ever before, whether by tapping into a local coffee shop's unsecured Wi-Fi network (easily sniffed by identity thieves) or making a purchase from a national retailer that relies on archaic data storage methods (easily compromised by hackers).

Organizations can be just as naïve about their own security. They may put too much trust in existing protocols, services, and components, or may not do enough to validate and monitor trusted relationships through available methods such as certificates, monitoring, and testing. Meanwhile, some businesses compliant with certain regulatory or industry standards assume meeting these standards ensures adequate security.

Ignoring known weaknesses is another problem for organizations. Consider that much of what was "new" in the way of threats during 2008 essentially came down to online criminals exploiting old problems—unpatched systems, weak security policies, and known vulnerabilities in the core infrastructure of the Web. By not addressing and patching existing issues, organizations cannot adequately prepare to combat new threats.

The threat against network operating systems has grown substantially over the past decade and recently, there has been a notable surge in criminal activity related to the exploitation of fragile networks. To fortify the networking and IT systems that make up their critical infrastructure, many organizations are now making such upgrades a part of their security strategy. In fact, some are viewing annual upgrades as being only a bare-minimum effort, and are conducting upgrades twice a year or more.

Another ongoing risk for organizations is people. For instance, employees can lose equipment, which can compromise sensitive data. Insiders looking to commit fraud also have more incentive today: The increase in data density makes attacks originating from within an organization much more profitable. Properly placed devices designed to sniff or collect sensitive data, or the copying of data that an employee has legitimate access to, are known to be at the root of several of 2008's high-profile security incidents.

Even hardware can pose a threat: Counterfeit chips inserted into computer equipment can obviously put sensitive data of individual users, businesses, and governments at risk. It may sound like fodder for a spy novel, but there have been reports of criminals (and even foreign governments) finding opportunities along the global supply chain to embed counterfeit components into devices.

While some experts say the security threat is overblown, counterfeit components can provide the "back door" that external parties need to access a user's personal information or monitor their communication. They are also extremely difficult to detect and can be costly to address. While software can be patched, counterfeit components must be removed one machine at a time.

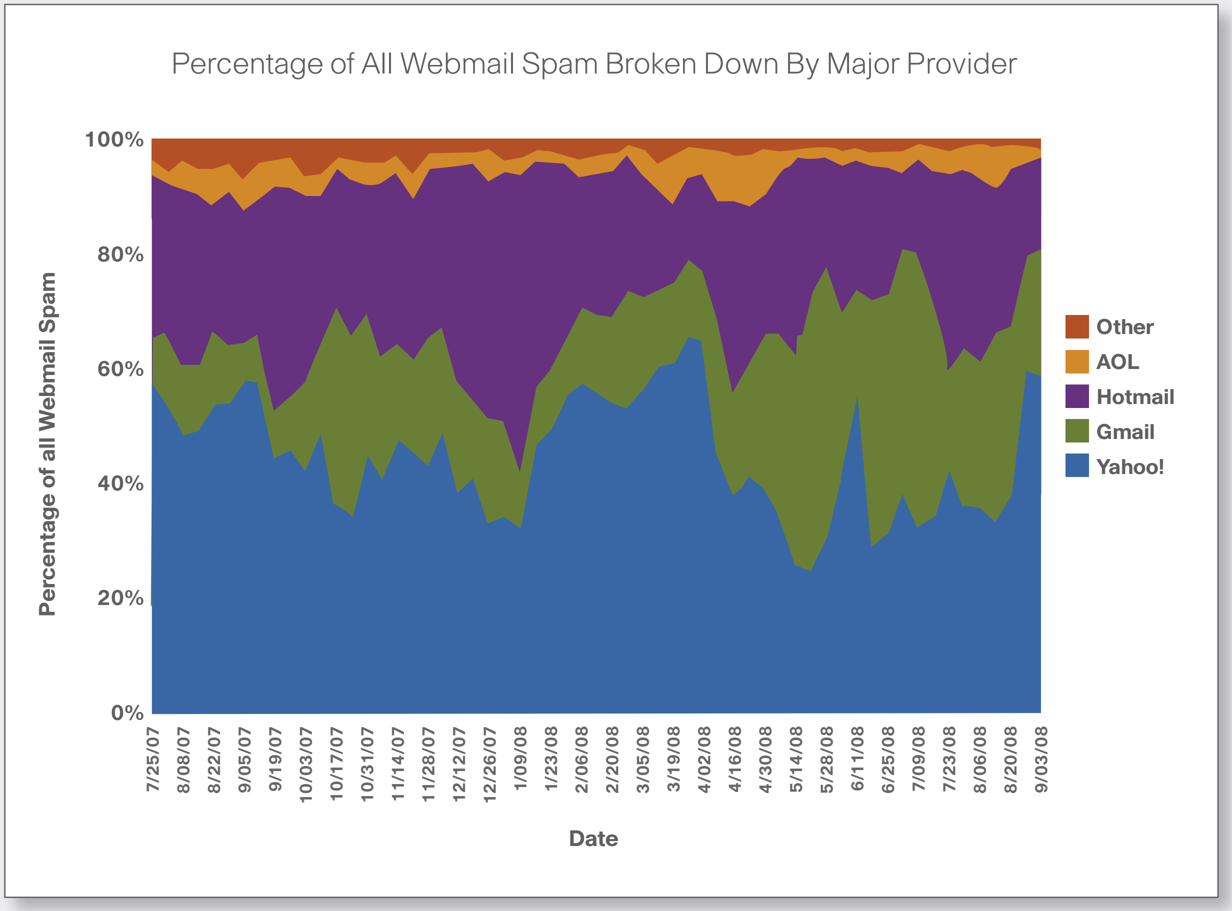
> Ignoring known weaknesses is another problem for organizations. By not addressing and patching existing issues, organizations cannot adequately prepare to combat new threats.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

New Tactics Erode Trust

Online criminals look for any and all favorable tactics to take advantage of users' trust—hence, the growing popularity of various kinds of reputation hijacking. In 2008, many leading companies with well-known and trusted brands had their reputations compromised by these attacks. Criminals successfully hijacked reputations by:

- Creating highly credible spam that appeared to come from a real company—both visually and by spoofing header information. Recipients were directed to legitimate-looking websites that were clever fakes.
- Overcoming security measures designed to avoid the mass creation of webmail accounts from top webmail providers with trusted reputations. Once criminals gained the ability to create large quantities of webmail accounts, they used them to send out massive amounts of spam, which was more likely to get through anti-spam filtering systems due to the legitimate webmail sender address.
- Poisoning DNS caches from local Internet providers so that typing in the legitimate URL would lead to a malicious site where users would provide sensitive personal and financial information.
- Inserting malware-downloading iFrames into thousands of legitimate websites (including those of major retailers and news organizations) through SQL injection and cross-site scripting, among other methods. A recent Cisco study estimates that 20 percent of all legitimate sites have been tainted by this type of attack.



The average spam rate from each webmail provider rose significantly for a period of time after tools to take advantage of their systems became commercially available.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Privacy and Trust Violations

More consumers are learning that their privacy may not be well protected by sources they trust. Businesses and organizations are freely sharing consumer information with third parties for advertising and marketing purposes. Often, they do not disclose that fact to consumers (or at least not as clearly as they should). Even when they do spell out policies, users may not read them (thoroughly or at all) before clicking "accept."

Sometimes, consumer data is put at risk when everyone in an organization does not fully understand the privacy protection practices, or when third-party vendors trusted with sensitive information are not aware of or do not follow security policies.

IT and privacy departments that establish strict policies around the use of customer data may find other departments undermining those directives. A 2008 Ponemon Institute study of executives shows that security and privacy officers responsible for protecting consumer data gathered by their organizations are clearly at odds with their own marketing departments, which share the same data (including email addresses) with external parties.

Universities, for example, gather and maintain a large amount of detailed personal and financial information related to their students and alumni. Last year, it came to light that many universities have been sharing this information with outside companies, including banks and credit card providers—a practice often in direct opposition to privacy protection policies, statements, and information provided directly to students.

Florida State University recently came under fire for providing names and addresses of students and alumni to Bank of America for a credit card promotion. The Consumer Warning Network (which obtained a copy of the contract) uncovered that, as part of the deal, the university receives a portion of every dollar charged by students and alumni on the credit cards, which feature the school's colors and logo. Florida State University reportedly is guaranteed to receive US$10 million over several years, and the money is being paid directly to the Seminole Boosters, a private entity that raises funds to support the school's athletic program—including paying coaches' salaries.

The irony of this situation: While doing this deal with Bank of America, Florida State University was simultaneously engaged in a media campaign warning its students of the dangers of credit card debt.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Vulnerabilities

Vulnerabilities exist in many technologies. Criminals take advantage of these weaknesses to install malware on computers and devices, gain control of computers and networks, and profit by making them parts of botnets or stealing sensitive data stored on them.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

To lower the risks of having criminals gain control over their systems, IT professionals and individual users work to find patches, fixes, and upgrades for the products and systems they use. It can look like a race between criminals looking for new or more attractive vulnerabilities to exploit and users trying to keep their systems patched and as secure as possible.

However, it can sometimes feel onerous to users to find and install patches or deal with the hassle of upgrading, and they may fall behind in keeping their systems and products patched and upgraded. This can be a real boon for criminals, as certain longstanding but not-always-patched vulnerabilities can offer easy ways of infiltrating systems.

The types of vulnerabilities most often exploited have changed over the years. Certain vulnerabilities are now more likely to be patched (sometimes automatically) as vendors have developed systems to both disclose and release patches for them.

In fact, Cisco found that the number of reported vulnerabilities in 2008 increased compared to 2007, growing by 6.77 percent. This continues the trend of previous years, and shows that vendors are more actively reviewing, identifying, and correcting vulnerabilities in their products. They're also more often collaborating with security researchers to do so.

According to the July 2008 IBM *Internet Security Systems X-Force Trend Statistics* report, security research organizations are finding nearly 80 percent of critical vulnerabilities. This correlates with Cisco information, which indicates that around 80 percent of critical vulnerability disclosures are coordinated with vendors of the affected products so that they can release patches or updates at the time of disclosure.

One result is that, while the overall number of disclosed vulnerabilities is rising, the number of "zero-day" vulnerabilities (vulnerabilities for which there is no patch available when exploit code is made public or discovered in the wild) in products such as major operating systems seems to be declining.

Another vulnerability trend is that many attacks now use a combination of multiple exploits that each target different weaknesses to increase the attack's access and control of the system. These combinations used in cross-vulnerability attacks can vary widely, depending on what operating system and programs are running on the targeted system.

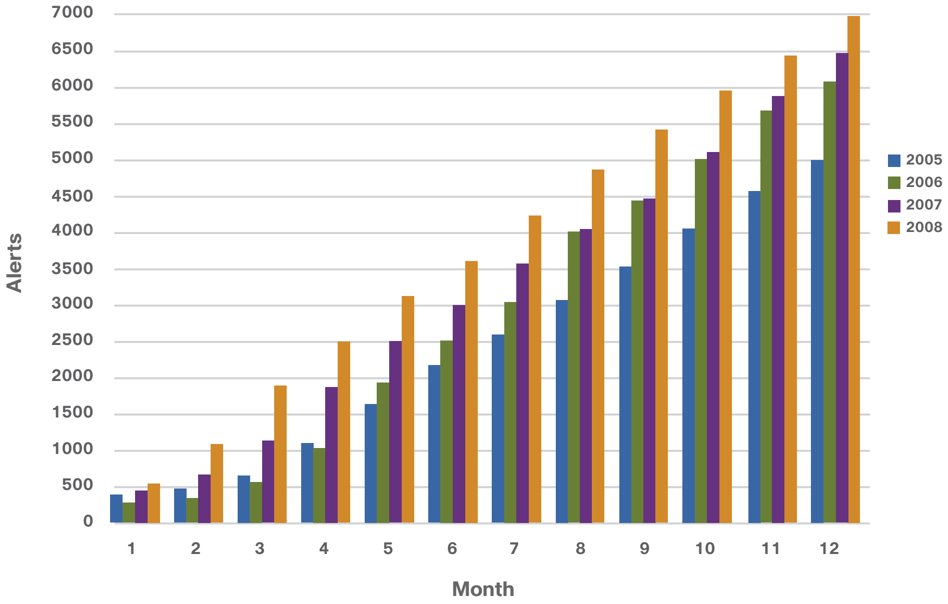
Web Vulnerabilities

With the Web being used by more people for more purposes in more new, untested ways, vulnerabilities along the entire Web ecosystem—including browsers, Web applications running in those browsers, servers, and some of the underlying infrastructure of the Web—continue to grow in number and importance.

And it's not just that new ways of use are creating new vulnerabilities. Many known vulnerabilities in Web-based tools and technologies continue to be exploited by online criminals. Some high-profile Web-based technologies known to have vulnerabilities include:

Adobe Flash Player. When users click on and view a malicious Flash file on a website or in an email, this can trigger the execution of arbitrary code with the privileges

Cumulative Annual Alert Totals



The number of reported vulnerabilities in 2008 increased compared to 2007, growing by 6.77 percent.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

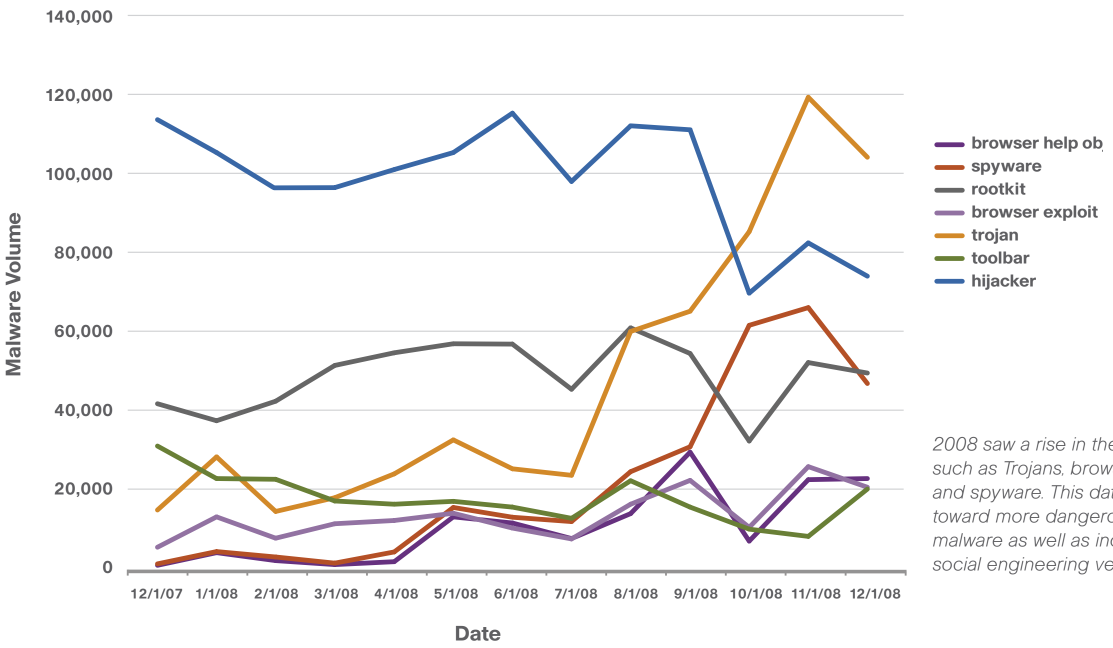
of the user. If the user is logged on to their computer with an admin account, the attacker could execute code that completely compromises the system. Widespread attacks using this vulnerability were conducted in April and May 2008. Adobe released updated Flash Player software in response, and multiple vendors updated their security settings and tools to stop this exploit.

WordPress. In March 2007, an entire version of this widely used blog-creation software was compromised when online criminals gained user-level access to a server hosting the latest official release of the software. They inserted malicious code into the then-latest official release. Anyone who downloaded and installed that version during the days it was up on the site ended up making their blog vulnerable to remote PHP execution by online criminals. In response, WordPress released a new version and hardened its servers.

Media players. Many popular media players used to play multimedia content that is either downloaded from the Internet or embedded in webpages have proven to be vulnerable to exploits. Vulnerable players include RealPlayer, Windows Media Player, Adobe Flash Player, and QuickTime. For online criminals, media players can be especially attractive to try to compromise, since users are conditioned to receiving messages that they should upgrade their media player to be able to play different kinds of content or for security. Sometimes these messages are legitimate, and may be ignored due to being viewed as a hassle, leaving the player vulnerable; other times these messages are attempts to exploit the media player to install malware on the user's computer.

> "With the increased complexity of many systems, entire classes of vulnerabilities can start to combine, so that individual vulnerabilities that may have seemed relatively harmless alone can turn into a serious risk factor when partnered with other threats."
>
> —Greg Spillman, Cisco Security Analyst

Different Types of Malware Detected (by month)



2008 saw a rise in the use of malware such as Trojans, browser helper objects and spyware. This data reflects a trend toward more dangerous, data-gathering malware as well as increasingly clever social engineering vectors.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Besides these well-known Web-based technologies that have proven to be vulnerable to attack, the growing crop of new Web 2.0 technologies such as widgets and add-ons for blogs and social networking sites may also be vulnerable.

There is also the risk that not all of these add-ons are well-intentioned. Developers have already been creating malware distribution, management, and support packages. Social engineering continues to be widely used by online criminals, many of whom have become aware of the value of social networks. Therefore, it seems logical that some of these developers would turn their attention to creating custom, highly appealing "mal-widgets" for social networking sites.

ActiveX Vulnerabilities

Vulnerabilities in ActiveX controls, which power many Microsoft applications and Windows applications, including the widely used Internet Explorer Web browser, continue to appear in very large numbers. Exploiting these vulnerabilities typically involves convincing a user to visit a malicious website that invokes a vulnerable ActiveX control.

Attackers used vulnerabilities in the Microsoft Snapshot Viewer, RealNetworks RealPlayer, Microsoft Help Visuals, and Computer Associates BrightStor ARCserve Backup ActiveX controls to conduct high-profile attacks in 2008. ActiveX vulnerabilities have also been used to propagate malware such as that which targeted outdated versions of RealNetworks RealPlayer for Windows. As evidenced by its success, users often have outdated versions of ActiveX controls installed. As in many situations, even though the vendor released an update to resolve the vulnerability, many users hadn't updated the software.

DNS Vulnerabilities

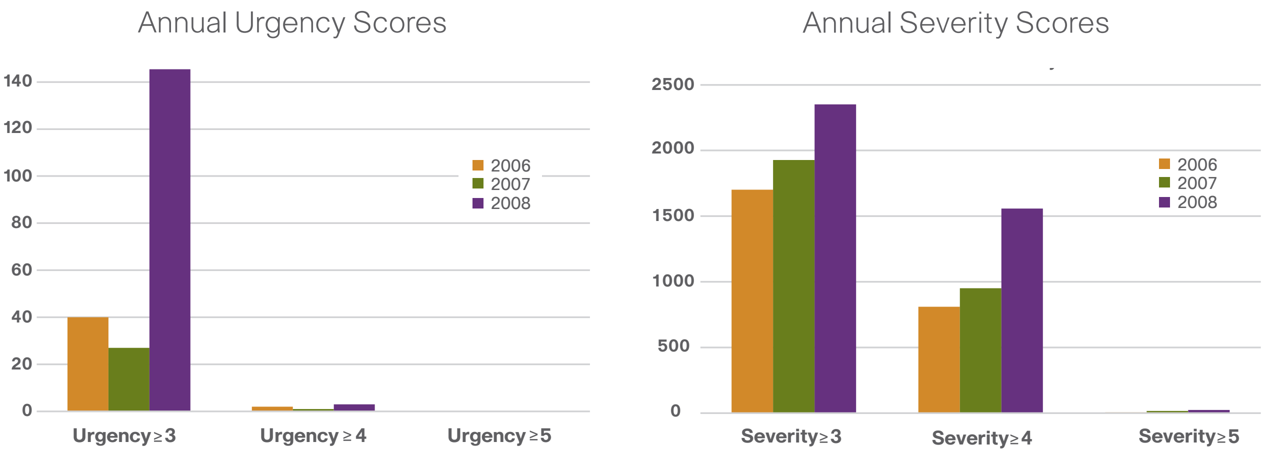
The big online security concern of 2008 may have been a Web ecosystem vulnerability that received extensive news coverage at the end of the summer. It involved vulnerabilities in a critical part of the Web's infrastructure, the Domain Name System (DNS) protocol.

The function of the DNS protocol is to resolve URLs and hostnames such as "cisco.com" to their numerical IP addresses, or IP addresses to URLs. The DNS protocol allows users to find websites by typing in "http://www.cisco.com" rather than "http://198.133.219.25". This makes it easy to associate domains and related subdomains with each other, even if the servers they are hosted on are not physically near each other.

DNS servers keep records of which domain names go with which IP addresses. When a DNS server receives a request to resolve a domain name in an IP address from a DNS client, it can look into the portion of the global DNS database it manages, or it can relay the query to other DNS servers that manage other portions of the global DNS database. To speed up their response time, DNS servers locally store responses they receive from other DNS servers in a local cache for a certain amount of time.

In an attempt to evade being blocked by IP address blacklists, botnet operators and other online criminals often take advantage of the DNS server's lack of restrictions on how frequently the records of a domain name and its associated IP address can be changed. Every few minutes, the malsite operators transfer the task of hosting a malsite from one botnet node to another. This practice is called "fast-flux," or domain-name kiting.

Worse, the DNS protocol itself—not just the lack of restrictions around changing the records in the DNS—has been shown to have exploitable vulnerabilities in the area of "cache poisoning."



These graphs show that both the urgency of vulnerabilities and threats (which is the equivalent of activity) and the severity (equal to the impact) are continuing to increase.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Recent Attack Using DNS Cache Poisoning

AT&T Internet Services. A DNS server resolving DNS queries for customers of AT&T Internet Services (formerly SBC) in the area of Austin, Texas, was compromised. It redirected AT&T Internet Services customers who tried to visit google.com to a malicious page that showed a fake version of the Google page and incorporated iFrame exploits.

The Importance of DNS

Almost everything the Internet is used for—not just the Web, but also email, FTP, voice over IP, banking transactions, and more—relies on the DNS. The DNS acts as the master map of the Internet. Users assume that map is correct, but if criminals can modify copies of that map, they can send anyone using that copy of the map (the DNS cache) to a completely unexpected destination, even while the users are being shown that they're following the map to their desired destination.

This is an especially crucial issue because the DNS is built to be distributed, with different DNS servers owning and trading different parts of the map. They update their parts of the map on a regular basis, but in between updates they use the stored versions of the map (their DNS caches) to send users querying that system to their destinations and give the stored versions of their part of the map to other DNS servers as guides to their neighborhood.

With the system set up as it is, a single point of failure—the compromise of even one DNS server—can allow an attacker to poison the cache and mislead all users querying that DNS server. And some of these DNS servers, for example, those of Internet service providers, serve and can potentially mislead millions of users.

DNS Cache Poisoning

DNS cache poisoning lets online criminals make a legitimate domain name redirect not to the IP address that domain name is supposed to be affiliated with, but to an IP address of their choice. That means they can control where Web users go, sending them to malicious websites even if these users never clicked on a malicious link and instead carefully typed in legitimate website URLs.

This makes cache poisoning perfect for hosting malware or for making phishing sites even more successful. Most "regular" phishing websites don't use legitimate URLs, but URLs that look very similar to the real URL; for example, a website in which the letter "l" in the domain name is replaced with the number "1"—making it hard for the visitor to detect that they are not actually visiting Mylegitimatebanksite.com, but instead My1egitimatebanksite.com.

Getting visitors to these fake sites usually requires using some kind of social engineering technique. But when criminals poison DNS caches, they don't need to use this subterfuge or send out spam linking to the not-quite-legitimate URLs. Instead, they use cached DNS records stored on DNS servers to control where Web users who correctly type in or click on a *legitimate* URL go. They essentially hijack all of the Web users who type in that URL (not just the smaller percentage that clicks on a link in an email or on another site), so that instead of ending up at the legitimate destination they typed in, the users are redirected to a malicious site.

For instance, typing in the legitimate URL Mylegitimatebanksite.com would not lead to that legitimate site, but could instead directly send users to a site that tries to download malware onto their computers, or one that looks similar to the bank's website but sends any information or passwords visitors type in straight to online criminals.

In mid-2008, major headlines were generated about a way of exploiting vulnerabilities in many vendors' DNS server software that could make it easier to poison DNS caches. Although DNS cache poisoning is not new, security researcher Dan Kaminsky identified a potentially more reliable and effective means of doing so.

For more information on DNS best practices, network protection, and attack identification, visit www.cisco.com/web/about/security/intelligence/dns-bcp.html.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

TCP Stack Table Implementation Vulnerability

Recently, a security researcher disclosed that both known and unknown weaknesses in the TCP stack table implementations of many products could be exploited using an exploit called Sockstress. Detailed research has not yet been released, but initial findings suggest that affected products could include most operating systems, routers, intrusion prevention systems (IPS), and firewall devices, since they all handle TCP traffic with stacks that could be affected.

The researcher is known to be working with vendors and organizations to assist in creating fixes for the affected TCP stacks. Depending on the time required to develop fixes, full information may not be released until sometime in 2009, when this vulnerability will undoubtedly receive additional attention.

Networking Equipment Vulnerabilities

Although many IT departments spend significant effort patching and upgrading desktop systems, applications, and data center equipment, upgrading networking equipment sometimes gets short shrift. This can be because if the network is working well, it doesn't seem like a good idea to interfere and cause network downtime—and upgrading networking equipment can be complex.

However, not implementing regular upgrades to networking equipment can be dangerous. The amount of research into vulnerabilities in networking equipment and operating systems increased in 2008, including for Cisco products. And if exploits do start showing up in the wild, the consequences of attacks on corporate networking equipment could be severe. Unscheduled downtime is one potentially painful consequence. Or worse, sophisticated attackers could leave the network running smoothly, and focus on compromising and gaining access to sensitive data residing all over the network.

Virtualization Vulnerabilities

Corporate environments are widely embracing virtualization. Whether virtual or remote workers, virtual data centers, or network virtualization, all offer benefits in the areas of cost-effectiveness and flexibility. Data center and network virtualization as well as "virtual client" products may also enhance ease of administration and security.

However, some of these virtualization products are still relatively immature, and have not been rigorously tested for security in live environments. This led to 103 vulnerabilities being exposed in virtual software products between January and November 2008. In that same time frame, major virtualization vendor VMWare issued 18 security advisories for its products in 2008, compared to seven advisories for all of 2007.

The increasing use of virtualization technologies in corporate environments is likely to make them attractive targets for additional attacks and exploits in the coming year.

> "As virtualization technology gains in popularity, it may bring with it new risks."
>
> —Don Simard, Commercial Solutions Director, U.S. National Security Agency in *InfoWorld*, March 13, 2008

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Encryption Vulnerabilities

The growing number of employees working from remote locations, the increased risk of data loss through error or malice, and the urgent need to protect important information make encryption a key security tool. Organizations are depending on encryption to secure email communications, shared data repositories, and devices such as laptops, CD-ROMs, flash drives, and other memory devices that include sensitive data.

However, several encryption technologies have shown vulnerabilities. And weaknesses in encryption can cause a false sense of security, with users and network administrators thinking they are protected from certain threats when, in fact, they are not.

In one high-profile example, certain versions of the open source operating systems Debian and Ubuntu contain an OpenSSL vulnerability that could lead to pseudo-random values being generated—and that could be easily predicted. Using these values could also generate weak encryption keys and certificates or passwords, which would then be vulnerable to brute-force attacks. At the end of August 2008, it became clear that online criminals were using stolen SSH keys to attack servers running Linux, and installing a malicious rootkit on them. There is speculation that the OpenSSL vulnerability in Debian and Ubuntu may have played a role in these attacks.

With many organizations using Linux-based servers—which this exploit laid open to control by online criminals—to run important parts of their networks, this was an extremely serious concern to many IT departments.

One encryption system known to be weak remains in widespread use: WEP, which is used for Wi-Fi networks. WEP was broken years ago, attack and exploit tools are widely available, and hacking into WEP-encrypted Wi-Fi networks is easy. Yet many individuals and organizations continue to use WEP, which leaves them vulnerable to criminal activity.

Organizations that process credit card information, such as merchants and service providers, will soon be required (by the 2008 update to the Payment Card Industry Data Security Standard) to upgrade from WEP to the stronger WPA encryption for their wireless networks. But the myriad organizations that provide free Wi-Fi access are not required to make this switch, leaving the security of their networks porous. Many home users of Wi-Fi access points also leave their networks vulnerable to snooping and exploitation.

Operating System Vulnerabilities

Although vulnerabilities that affected all major versions of the Microsoft Windows OS and the Linux kernel showed up in 2008, overall, the number of OS vulnerabilities discovered declined compared to previous years. Most of these vulnerabilities require user interaction; very few are exploitable by unauthenticated remote attackers if the victim does not open a file or otherwise perform a required action.

Widespread acknowledgement of the importance of patching and regularly updating operating systems—and making patching easier—have significantly contributed to the decline in OS vulnerabilities. Microsoft's efforts in this area have been quite successful. So although OS vulnerabilities are still being reported, their decline indicates that attackers are increasingly looking to other classes of vulnerabilities to compromise systems and user information.

> "The more complex the threats become, the more you have to do the basics and groundwork *really* well. Staying aware and on top of new vulnerabilities and ensuring that patches and software updates are rapidly implemented is crucial."
>
> —Jeff Shipley,
> Cisco Intelligence Collection Manager

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Vulnerabilities in Databases and Office Productivity Applications

The use of vulnerabilities in office productivity applications to conduct both targeted and widespread attacks continued in 2008. High-profile malicious code attacks involved products such as the Microsoft Office suite, Microsoft Jet Database Engine, Adobe Acrobat, and Ichitaro word-processing software from Japanese office productivity tools vendor JustSystems.

Interaction from the victim—for example, opening an attached document or malicious database file—is typically required for criminals to exploit these vulnerabilities and take control of targeted computers. Once attackers have control of the user's system, they could bypass certain perimeter defenses on a corporate network and launch additional attacks.

Files associated with these types of applications are well-suited for targeted attacks by knowledgeable attackers using social engineering techniques. For instance, an attacker might send a malicious spreadsheet labeled "Profit and loss statement for shipping department" to people in an organization's accounting group. The attacker could spoof the origin of the document by using easily found information from a corporate website, such as the names and email or physical addresses of executives. This is especially effective as spreadsheets and other office productivity files are commonly used in organizations for legitimate business. That means that users often trust them, and they're rarely blocked at the network perimeter.

Mobile Device Vulnerabilities

The BlackBerry, an essential part of modern workplace productivity, suffered from a vulnerability this year that could compromise corporate networks. Research In Motion (RIM), the makers of the BlackBerry, disclosed that the way these devices open PDF attachments could leave corporate networks vulnerable to being compromised.

Other smart phones are vulnerable as well. Weaknesses in installer applications have allowed Trojans to be installed on certain phones. And the Web browsers that some mobile phones use may make it easier for users to fall victim to phishing campaigns. For example, a mobile phone's Web browser may be configured so that the address bar doesn't show all of a long URL. With phishing sites, the first part of the URL often looks legitimate, but the latter part may give clues (an "off" top-level domain, or strings of numbers) of being a phishing site. Or the mobile phone's input method may make the process of manually entering URLs into the address bar arduous, so that users are more often tempted to "just click" on a possibly malicious link.

As with Web 2.0 technologies, some smart phones offer an open application development environment, which means that downloading a new application for the phone carries the risk that it might be malware. Or, if it wasn't developed using secure coding practices or thoroughly tested before release, it might merely be easily exploitable.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Geopolitical and Political Conflicts

Spam, malware, and botnets are being used to a greater extent as weapons in geopolitical and political conflicts, as in Estonia in 2007 and Georgia in 2008. It is estimated that this trend will continue in the years to come.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

In the 2007 "Estonian Cyberwar" (said to have been a revenge attack in response to the Estonian government's removal of a statue of a Russian soldier from a prominent location in the capital), Estonian government, banking, and media websites were attacked and shut down using botnet-based DDoS attacks. Speculation continues about whether these online attacks were spontaneous, or occurred with Russian state backing.

In July 2008, in the weeks leading up to and during the Russian-Georgian conflict, Georgian government websites were defaced or shut down, as was the website of the National Bank of Georgia. According to reports in the *International Herald Tribune*, attacks were hosted out of servers in the U.S. as well as Russia, attesting to the flexibility of "cyber-warfare." Botnets affiliated with the Russian Business Network, a group of online criminals with ties to the Russian government, were used in the attack.

The Burmese junta has also used online methods against those protesting its regime. During the 2007 political protests in Burma, the junta shut down all Internet access for the country. (Burma has only one ISP, owning satellite phones is forbidden, and computers in Internet cafes log user activities by automatically taking a screenshot every five minutes.) This attempt to stop protesters from sending out digital photos and reports of the political protest was largely unsuccessful, so on the anniversary of the protests in September 2008, the junta reportedly used DDoS attacks to shut down dissident websites.

In many of these cases, it is and will remain very difficult to prove state backing of DDoS attacks against enemy websites. However, from a security perspective, being aware that geopolitical conflicts are more likely to include an Internet component—whether it is state-sponsored, or actions from individual hackers—can help organizations prepare for the chance that DDoS attacks may be used against a country's government, financial, media, or vital infrastructure websites.

In an interesting political twist, the 2008 U.S. election also saw DDoS attacks against the websites of certain political campaigns, such as that on a website urging votes and soliciting donations to counter a high-profile proposition banning gay marriage in the state of California. Using a DDoS attack, proponents of the proposition were temporarily able to deny visitors access to the opposition's website and impede their ability to donate money to its campaign during a fundraising drive.

Awareness that botnet activity is likely to increase during geopolitical and political conflicts may also be helpful in creating a proactive security strategy. And the apparent weakness of many state-run networks is important to address. If security professionals at these organizations remain alert to the fact that their networks and websites may become targets during conflicts, they may be able to strengthen their networks earlier and more thoroughly. For example, they could proactively monitor online discussions of techniques that may be used against them, allowing them to counter attacks with patches and workarounds.

> "You could fund an entire cyber-warfare campaign for the cost of replacing a tank tread, so you would be foolish not to."
>
> —Bill Woodcock, *Packet Clearing House* in *The New York Times*, August 13, 2008

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

From Conflicts to CyberCommands

For many years now, what could be termed low-level cyber-warfare has existed between semi-organized hacker groups with political, religious, and other motivations—for instance, between Israel and Palestine, China and Taiwan, India and Pakistan, and others. A recent change is the addition of overt state sponsorship and military backing for Internet-based warfare.

The escalation of cyber-warfare from semi-organized individuals or groups to state-sponsored activities brings a new level of resources, capabilities, skills, and organization to this arena. The governments of several countries, including the U.S. and China, have set about establishing "cyber-command" organizations. These organizations are tasked with protecting their respective countries from online warfare and with creating offensive cyber-warfare capabilities.

Even though more countries are pursuing this, there is an ongoing debate (often outside of military circles) about whether or when an offensive cyber-warfare capability is warranted or a sound decision. That is the experience of many network administrators has shown that trying to go on the offensive against Internet attackers seldom proved to be a sound, responsible, or fruitful decision.

Cyber-warfare has not been well-defined except as an extension of existing electronic warfare; interception and exploitation of communications would certainly be included under this concept. For example, in mid-2008, unclassified White House emails were exfiltrated, according to FBI sources. Origins of the attacks were traced back to servers in Russia and China, although the existence of state backing is difficult to prove. Security firms linked to the campaigns speculated publicly that foreign entities may be pursuing a "grains of sand" approach, in which large amounts of less-well-protected data is being carefully sifted for nuggets of important information.

In this context, it is interesting to note that governments around the world are implementing many privacy and wiretapping laws, or granting immunity to the telecommunications firms that enable wiretapping. Recent examples include a proposed U.K. law that would allow the government to collect data on all electronic communications. Another U.K. proposal would require user registration for all mobile phones, allowing the government to create a central database of all U.K. mobile users. Notwithstanding significant popular opposition to these proposals, this indicates an ongoing commitment to more closely monitoring communications that may have security implications. In many countries, average citizens will not be affected by this monitoring, unless there are security implications, such as international phone calls to countries or individuals of concern to state authorities.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Countering Internet Security Threats

Apart from working to minimize vulnerabilities and fighting back against current Internet security threats on a case-by-case basis, several broader initiatives are also being used in the battle for online security.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

DNSSEC

Industry and governments are working hard to mitigate DNS vulnerabilities—the hot issue of summer 2008. Implementing Domain Name System Security Extensions (DNSSEC) is widely seen as crucial to ongoing Internet security, in that DNSSEC will provide integrity of DNS information to protect against spoofing and cache poisoning exploits.

Although most experts agree that deploying DNSSEC is crucial, adoption faces several challenges, such as implementation complexities and disagreements over who should own the top-level root keys. The top-level country code domains of Sweden, Bulgaria, Puerto Rico, and Brazil already use DNSSEC. And U.S. officials recently announced that DNSSEC would be implemented for the .gov domain by January 2009, and for all .gov subdomains by December 2009, which should further spur worldwide adoption.

Security vendors and researchers are collaborating more closely on the disclosure of vulnerabilities, so that patches and workarounds can be created before the exploitable information is widely available. Security vendors are also working both together and separately to make it easier to report and discover current security incidents, and to assess threats accurately. Government initiatives designed to enhance security are being implemented in several countries. And law enforcement is working to send online criminals to jail.

Industry and Government Initiatives

In two separate incidents, hosting providers for online criminals were shut down (InterCage in September 2008 and McColo in November 2008), thanks to efforts by security researchers or organizations, law enforcement, or ICANN. In both cases, the amount of spam sent out worldwide decreased noticeably for several days, until the hosting providers' clients found other providers. Although the long-term impact was limited, this was a positive step: Industry and law enforcement organizations were able to identify and collect evidence showing the malicious activity, and more importantly, positive action was taken by higher-level service providers to InterCage and McColo and organizations like ICANN.

There are other recent examples of law enforcement and courts working to stop or prosecute online criminal activity.

- In July 2008, Seattle "spam king" Robert Soloway was sentenced to 47 months in prison. Notorious for marketing spamming services that used botnets to send billions (or by his own account, trillions) of spam emails, often with spoofed headers that made it appear as though they came from Hotmail or MSN accounts, Soloway finally pleaded guilty to mail and email fraud.
- British hacker Gary McKinnon may be extradited and tried in the United States on charges of hacking into NASA as well as U.S. Pentagon, Army, Navy, and Air Force computers. McKinnon claimed he never harmed the computers, but was looking for evidence of alien technology.
- A U.S. District Court, acting on information collected by the Federal Trade Commission (FTC), shut down and froze the assets of a major international spam network known as HerbalKing. HerbalKing sent out billions of spam messages to market potentially unsafe versions of prescription drugs. The FTC received more than three million complaints about messages related to this operation. The court froze the spam network's assets and issued a temporary injunction that prohibits the defendants from sending spam and making false product claims. New Zealand authorities, working with the FTC, also took legal action against the spammers, and the U.S, government is planning to pursue criminal charges.

On the industry and government collaboration front, new organizations such as the Industry Consortium for the Advancement of Security on the Internet (www.icasi.org) are addressing multi-vendor global security threats and creating a forum for industry collaboration and innovation around security.

And industry standards continue to be updated to reflect changes in technology and security. The Payment Card Industry Data Security Standard (PCI DSS), for example, was updated in 2008 to mandate more secure wireless encryption technologies.

Meanwhile, National Computer Emergency Response Teams (CERTs) continue to play valuable roles in assessing threats and vulnerabilities, providing information on them, and coordinating vendor response, as do other government and industry associations.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

In the area of identity theft, the U.S. government's 2008 Identity Theft Task Force Report indicated that in 2007, 2470 criminals were charged with identity theft-related crimes, while 1943 were actually convicted. The high rate of conviction for those prosecuted, combined with compliance requirements and more organizations following best practices around safeguarding personal information, is helping to reduce the likelihood of identity theft.

Yet criminals can still make large profits from identity theft-related crimes while the probability of prosecution is currently low. (To ensure sufficient prosecution of such crimes, the report recommended that the government review its civil monetary penalty programs.)

More thoroughly tackling identity-theft-related crimes will require a comprehensive approach toward ensuring greater individual awareness and additional security measures by businesses, as well as prosecution and international cooperation. To make further progress, increasing the reporting of such crimes to and cooperating with law enforcement will be especially important.

Enabling Technologies

Security vendors are actively working to make security simpler, which helps to enhance the implementation of and adherence to security tools and policies.

For example, vendors have been disclosing threats and releasing patches more quickly. And to help with crucial user education efforts, many vendors have been making it easier for end users to find information about security risks and threats and to assess their potential negative effects.

For many vendors and users, making security simpler with technology means creating security solutions that:

- Make it easy to establish and adapt security policies
- Automate security tasks (such as encrypting sensitive data or deploying patches)
- Offer protection within, as well as at the edges of, the ever-expanding network
- Closely monitor and assess threats in real time
- Protect from threats along multiple vectors
- Integrate with other security tools
- Empower workers to safely use new collaboration and productivity tools

Making Security Easier to Find

A useful industry standard was created to make it simple to report security incidents and discover information about current security issues. This involved having companies create a standardized high-level "security" page on their websites, with a location that would be easy for visitors to remember. So, a user wanting to see the latest information about a known vulnerability that affects products from a company known as Example would just need to type "www.example.com/security" into a browser. Although some companies have implemented this standard, many are still lagging.

Standardized Security Page
cisco.com/security
microsoft.com/security
adobe.com/security
yahoo.com/security
facebook.com/security

Not Yet
apple.com
secondlife.com
google.com
mcafee.com
myspace.com

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Conclusions and Key Recommendations

2008 marked both an expansion and evolution of the online security threat landscape. In some cases, online criminals reaped rewards of tens or hundreds of millions of dollars. This potential for profit will continue to drive nefarious innovation and specialization in the year ahead.

Threats that combine one or more online elements—the Web, spam, malware, and botnets—continue to grow in number and sophistication. For greater effectiveness, criminals are more and more often targeting specific individuals or groups and exploiting legitimate websites and other trusted entities and systems. They are launching increasingly hard-to-detect threats that can dupe even savvy, cautious users. And they use social engineering techniques and take advantage of current events to make their online schemes appear highly credible or appealing to their victims.

Meanwhile, the malware that is spread through online threats is constantly being redesigned to be smarter and more surreptitious than ever before—and it has an enormous growth rate. Botnets, the core of criminal activity on the Internet, continue to spread malware, send out millions of spam emails, host malicious websites, and attack legitimate ones. To counter these threats, organizations should include active anti-malware and botnet prevention components in their security strategies.

Online criminals are exploiting both old and new weaknesses in technologies and systems to create botnet armies. Known high-impact vulnerabilities are going unpatched. At the same time, increasing use of mobile devices and remote working, Web 2.0 tools, virtualization, and new forms of collaboration are all expanding the security perimeter and making the edges of the network more permeable. This poses a significant challenge when organizations try to shore up their defenses, and underscores the need for adoption of advanced security policies and technologies.

Data loss continues to be a challenge that can have grave, costly effects on organizations and individuals. Creating strong security policies can help, but these policies must be implemented and enforced throughout the organization. Regarding data loss, many organizations now assume that company equipment with sensitive information is likely to go missing at some point. As a result, they are also increasingly using tools and technology—including virtual private networks, content filtering at the gateway, authentication technologies, access controls, encryption, and data removal and truncation—to keep sensitive information from being accessed or used by unauthorized persons.

Insider threats are another issue that requires awareness and vigilance. In a troubled global economy, more of these attacks can be expected.

On the upside, expect to see more news stories in 2009 related to how authorities are combating offenders and spammers. By offering specialized, complex services, modern offenders are becoming more established, and tracking and catching them may become easier. However, even as security vendors and authorities collaborate to bring online criminals to justice, this does little to diminish the number of attacks.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Putting IT on the Front Lines

According to Cisco's August 2008 InsightExpress report, *The Challenge of Data Leakage*, approximately 50 percent of business workers worldwide mix business and personal use on their computers. For most companies, the blending of business and personal IT use is inevitable, but it makes defining and enforcing acceptable use policies that much more challenging.

In fact, a recent study by Cisco of the common failures of enterprise security policies revealed gaps between IT's perceptions of why policies are violated, and employees' true motivations. Most employees surveyed said they broke security policies because the policies either did not align with the realities of their jobs, or they needed to access applications not included in the policy, or both. Yet most IT professionals thought apathy and lack of awareness were the typical reasons for employees' security policy violations.

Many companies are struggling to define acceptable use policies that enhance security, but are not so inflexible that they stifle collaboration and the art of getting business done in today's highly competitive, Web-enabled world.

IT personnel can help with this, and should be at the forefront of combating security risks. According to the *2008 Global Information Security Workforce Study* from Frost & Sullivan, qualified and experienced personnel are the key to stopping security threats. They can work directly with management and employees to create and implement relevant and user-friendly policies that are practiced throughout all levels of the organization, starting in the boardroom.

But, if IT is to be more involved and effective at helping to ensure security across the enterprise, organizations must invest more in their IT departments. Ensuring that IT departments can access adequate resources and the most knowledgeable and experienced professionals—particularly, security specialists —is key.

It is also important to change the perception of the IT department's security policies from "forbidding" to "empowering." For example, when IT personnel recognize that employees will download the tools they want regardless of IT policies, they can offer realistic solutions to the problem, such as providing vetted versions of downloadable tools and creating secure pathways to content on work-related Web destinations.

When employees do inevitably make a mistake or inadvertently download something that compromises security, they should be encouraged to be open about it with IT so the issue can be addressed quickly. If the incident is the result of simple human error, without malicious intent, organizations should take a stance of demonstrating appreciation to the employee for helping to swiftly identify and combat the threat. This will encourage users not to feel fearful about informing the IT department about risks.

Employees can play a vital role in safeguarding their own online identity and understanding the risks that go hand-in-hand with their use of technology. Ongoing user education around security policies and technologies and online threats can help. An important benefit of companies educating and training their workforce about security risks and threats: It can ultimately lead to better technology practices in the employees' personal lives, thereby helping to keep online criminals at bay on two fronts.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Key Recommendations Checklist

✓ Stay focused.

✓ Stop users from inadvertently downloading malware onto the network.

✓ Patch known vulnerabilities.

✓ Prevent data loss.

✓ Take insider threats seriously.

✓ Remember the network.

✓ Think beyond compliance.

✓ Make security simpler.

Key Recommendations

Stay focused. One essential thing for organizations to keep in mind about security is that when they try to protect *everything*, nothing will be protected. Instead, organizations should focus most of their time, energy, and resources on what is strategically, financially, and competitively most important to safeguard.

Stop users from inadvertently downloading malware onto the network. To ensure that users cannot visit—or download the compromised parts of—webpages that contain malware, use several malware scanning technologies; proactive, real-time, reputation-based filtering solutions; and rule- and application-based firewalls and intrusion detection and prevention software at the network gateway.

Individual users can also significantly reduce their chances of falling victim to malware downloads. Keeping browsers fully updated and patched, using security features and settings, and remaining aware of existing and emerging threats is crucial, as is never clicking on a link received in email—even email from apparently trustworthy sources. Instead, users should always manually type in a trusted URL, bookmark it, and revisit it by using the bookmark rather than by clicking on links provided by others.

Patch known vulnerabilities. To be effective in today's landscape of evolving threats, security organizations must be aware of new trends. However, many current and emerging threats take advantage of *known vulnerabilities*, so organizations should not become wholly distracted by emerging threats. Spending time, energy, and resources on addressing and patching existing defects in their security armor remains essential.

Around 80 percent of common attacks take advantage of 20 percent of high-impact vulnerabilities. These high-value vulnerabilities are often very basic, and continue to be unpatched in certain environments. Staying up-to-date on these high-value vulnerabilities (and securing them) will, in most cases, lead to a good "80/20" solution.

Prevent data loss. Strong security policies are essential for protecting an organization from the negative effects of data loss. But these policies must be enforced to be effective, and users must be made aware of them.

Recommendations for reducing the risks associated with data loss include:

- Deploy methods (preferably automated) to maintain the confidentiality of information on mobile devices such as laptops, thumb drives, and PDAs through methods such as access controls, encryption, remote data removal, data association, redaction, truncation, or other methods that effectively render data unusable.
- Classify data and put stronger controls on what data people can access.
- Define which data should be protected, so that the focus is on keeping the most critical information the most secure.
- Educate users about what information should not be stored on a laptop or other mobile device, and what to do if such equipment is stolen.
- Actively monitor email and Web traffic to ensure that sensitive information is not being shared inappropriately.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Take insider threats seriously. Be vigilant by continually logging, auditing, and monitoring traffic patterns, systems, and databases. Set policies that prevent employees from engaging in unauthorized activities. Businesses should ensure that their information security teams coordinate with physical security teams and HR departments to implement effective policies for revoking access of terminated or transferred employees. Always conduct thorough background checks during the hiring process.

Remember the network. Enterprise security is not just about headline-grabbing malware threats and data breaches. Despite being a security blind spot for many organizations, network devices are at risk, too. Many organizations use an “if it’s not broken, don’t fix it” approach to their networks—especially in a cost-conscious, down economy. While most organizations should upgrade their networks at least once a year, the optimal upgrade frequency depends on size, complexity, security requirements, resource constraints, and other considerations.

Think beyond compliance. Organizations should not let compliance be a security placebo. By focusing almost exclusively on compliance, and aligning their procedures to meet those requirements, organizations can lose sight of the current, rapidly evolving risk and threat environment. In addition to reviewing compliance levels, organizations should conduct regular top-down gap analyses to augment existing procedures and proactively meet current and emerging threats.

Make security simpler. Above all, make security tools and solutions easier to implement and use, and make security policies easier to follow.

- Layer integrated sets of security technologies, rather than depending on patchwork and point solutions.
- Ensure that security solutions and departments effectively share data.
- Set security policies that protect all important assets, and make their implementation automated and straightforward.
- Teach IT departments and employees to work together to enable safe access to productivity-enhancing tools and content—both within and outside corporate networks.
- Keep existing network and security hardware and software patched and updated in ways that don’t impede productivity.
- Work continuously on user education and awareness of new threats, and encourage users to report possible or suspected gaps in security.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Top Trends to Expect in 2009

To help organizations develop their security strategies and plan their IT budgets for 2009, Cisco has identified the following key trends to watch for in the year ahead. These predictions are based on news and events from 2008, as well as related information and insight provided by Cisco's security and business operations worldwide.

Smaller, More Frequent, Targeted Attacks

More sophisticated attacks will occur in the year ahead. They will be deployed rapidly and designed for even more specific targets—individuals, groups, businesses, organizations, and governments. The current worldwide financial crisis is still playing out, natural disasters and manmade strife will continue to provide global news hooks, and a new U.S. president is taking office in 2009. Criminals will certainly keep refining how they take advantage of (and profit from) these types of news events.

Social engineering and phishing techniques have been profitable, so offenders can be expected to keep refining the delivery method for (and improving the success of) these attacks. There will be more "specialists"—criminals who deliver one or more key components essential to creating a complex and convincing attack. As they grow their expertise and reputation, these specialists will be sought out and hired by others looking to create their own high-impact attacks.

Cross-Protocol Attacks

Online criminals looking to improve their odds of success will increasingly rely on cross-protocol or "blended" approaches that combine email, Web-based threats, and intrusions. This type of attack, successful in recent years, will keep growing during 2009. Also expect to see more botnets that are capable of "multitasking"—for instance, sending spam, hosting malware, *and* launching a direct attack.

To defend against more robust multi-protocol attacks, organizations will need to implement security systems that can monitor all Internet traffic types and rapidly identify and stop new threats. Security solutions that focus on only one area (such as email, IPS or Web-based threats), or those that cannot effectively correlate data between areas, will not be enough to protect organizations from blended threats.

Reputation Hijacking

Hijacking reputations has proven attractive and effective for online criminals. When people trust a brand, they are likely to visit an associated site or open an email from that source without question. Many traditional or point security solutions depend on URL or IP filtering lists and don't have real-time insight into traffic patterns and suspicious behavior from every element on a webpage; these solutions are not equipped to recognize that a trusted website or email sender has gone bad.

In 2009, more online criminals will be actively hijacking reputations and will work on finding additional, more sophisticated ways to do so.

Mobility, Remote Working, and New Tools as Risk Factors

The trend of remote working and related use of Web-based tools, mobile devices, virtualization, "cloud computing," and similar technologies to enhance productivity—especially in an economic climate that demands leaner, more-cost effective and global staff—will continue in 2009.

This means that preventing loss of data—from outside attacks, insiders, or negligence around data storage devices such as laptops—will become more crucial than ever. But it will be a challenge for security personnel. The edge of the network is expanding rapidly, and the increasing number of devices and applications in use make the expanding network more porous, creating new inroads for threats.

Organizations of all types should implement thorough, sensible data loss prevention (DLP) policies and consider security solutions that automatically prevent sensitive data from leaving protected environments.

Every organization should also begin to take simple steps designed specifically to protect intellectual property—an increasingly precious asset in the modern economy.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

A Holistic Approach to Security

Cisco's vision for security is enabling customers to collaborate with confidence. To do so, Cisco champions a holistic, proactive, layered approach to counter existing and emerging security threats.

Cisco Security Intelligence Operations is an advanced set of capabilities that provides threat detection, correlation, and mitigation to continuously enable the highest level of security for Cisco customers. Using a combination of a team of global research engineers, sophisticated security intelligence, and automated update systems, Cisco Security Intelligence Operations allows customers to securely collaborate and embrace new technologies.

With the increase in blended, cross-protocol, and cross-vendor vulnerability threats, the security industry has come to recognize that point defenses that protect from individual threats or protect individual products are no longer enough. Integrated security management, real-time reputation assessment and a layered, multi-point approach are the new watchwords.

Cisco Security Intelligence Operations will use tightly integrated data derived from multiple Cisco divisions and devices to continuously assess and correlate Internet threats and vulnerabilities. Sources of this data include:

- **Cisco's worldwide Threat Operations Centers**, at which over 400 researchers track new trends and threats.
- **Cisco Security Remote Management Services**, a 24-hour-a-day, 7-day-a-week team of highly-certified, experienced security and network professionals who provide operational support for security incident monitoring, fault and performance incident management, problem resolution, security infrastructure tuning, and secure network access control support.
- **The SenderBase Network**, which monitors 30 percent of all Web and email traffic worldwide and handles 30 billion queries every day. To assess the real-time reputation and trustworthiness of every active Web server on the Internet, the SenderBase Network tracks more than 150 different network-level parameters.
- **Cisco Security IntelliShield Alert Manager**, a customizable alert service that provides up-to-the-minute, actionable intelligence, in-depth vulnerability analysis, and highly-reliable threat validation.
- **Cisco Intrusion Prevention Systems**, which identify, classify, and stop known and unknown threats, including worms, network viruses, application threats, system intrusion attempts, and application misuse.
- **Real-time network traffic telemetry data** provided by Cisco network devices, which will be implemented in Cisco products starting in 2009.
- **A variety of other Cisco functions,** including Cisco Security Research and Operations, Cisco Security Incident Response, the Corporate Security Programs Office, and Global Policy and Government Affairs.

With Cisco, organizations can save time researching threats and vulnerabilities, and focus more on taking a proactive approach to security.

As Internet threats continue to evolve, Cisco Security Intelligence Operations will enhance Cisco's ability to identify global threat activities and trends, and provide expert analysis and services to help protect users from these threats. Cisco is committed to providing complete security solutions that are integrated, timely, comprehensive, and effective—enabling holistic security for organizations worldwide.

All contents are Copyright © 2008–2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

For More Information

Cisco Security Center
www.cisco.com/security

SenderBase
www.senderbase.org

Cisco Security Solutions
www.cisco.com/go/securitysolutions
www.cisco.com/go/ros

Cisco Security Products
www.cisco.com/go/security
www.cisco.com/go/intellishield
www.cisco.com/go/ips
www.ironport.com

Cisco Corporate Security Programs Organization
www.cisco.com/go/cspo

Report available for download at
www.cisco.com/go/securityreport

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at **www.cisco.com/go/offices**.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

Cisco 2009 Midyear Security Report

An update on global security threats and trends

Introduction

The Cisco® Midyear Security Report presents an overview of Cisco security intelligence, highlighting threat information and trends from the first half of 2009. The report also includes recommendations from Cisco security experts and predictions of how identified trends will evolve.

As the global economy struggles to regain its footing, one moneymaking sector remains healthy—online crime. This sector embraces technical innovation, collaborates with like-minded enterprises to develop new strategies for generating income, and continues to demonstrate adoption of the best legitimate business strategies to maximize profits.

Criminal sophistication and business acumen have increased since the publication of the *Cisco 2008 Annual Security Report*. For instance, criminal enterprises are innovating new business models with the creators of botnets—networks of compromised computers that can carry out the bidding of online scammers. These innovations include "botnets as a service," a sobering spin on the software-as-a-service trend that has spread across the technology sector.

"We see many signs that criminals are mimicking the practices embraced by successful, legitimate businesses to reap revenue and grow their enterprises," said Tom Gillis, Vice President and General Manager of Cisco Security Products. "It seems the best practices espoused by *Fortune* magazine and Harvard Business School have found their way into the online underworld."

Cause for Concern: Technical Innovation of Online Criminals

The technical innovation and capabilities of online criminals are remarkable. The Conficker worm, which began infecting computer systems in late 2008 and early 2009 (and is still infecting thousands of new systems daily), provides the best example. Several million computer systems have been under Conficker's control at some time as of June 2009, which means the worm appears to have created the largest botnet to date. (Read more about Conficker on page 4.)

Security industry watchers also point to the methods used by Conficker to propagate and create the botnet. Instead of using newer approaches that involve social engineering, or delivering the payload via email or the Internet, Conficker's creators exploited a vulnerability in the Windows operating system. This was an "old-school" method that may not have seemed threatening, given the preponderance of new tactics for online scams. Conficker's creators appear to have recognized that their entry point into computer systems might yield more satisfying results.

It's safe to say online attacks will continue to showcase the most cutting-edge technology—and criminals will try to use older tactics in new ways. Criminals are also closely watching security researchers and learning from their methods for thwarting attacks, putting the "good guy" knowledge to use so their next attack can evade existing protections.

Cause for Concern: Criminal Sophistication and Collaboration

"Bad guys" are aggressively collaborating, selling each other their wares, and developing expertise in specific tactics and technologies. Specialization makes it tougher to shut down illegal activity, because there are many players in this ecosystem.

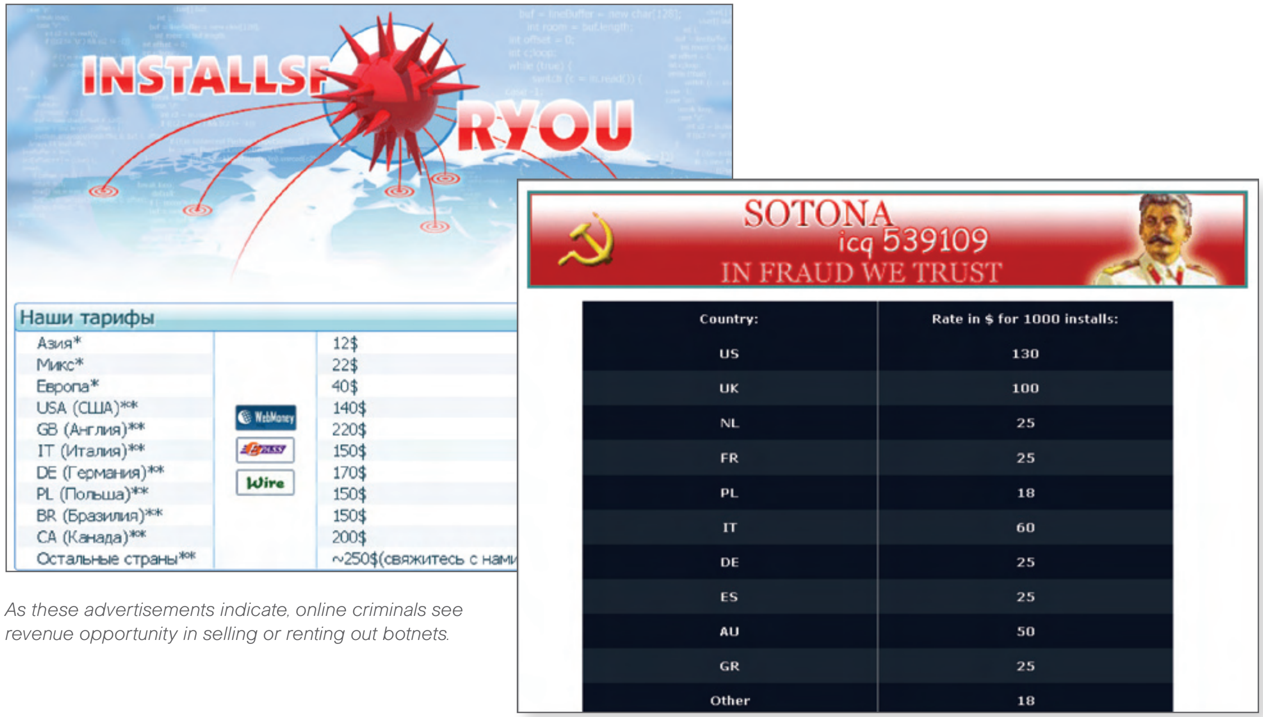
Consider the collaboration between the creators of two large botnets, Conficker and Waledac (see page 10). In April, the Conficker botnet monetized itself by delivering the Waledac malware via Conficker's own hosts, along with scareware—scam software sold to consumers based on their (often unnecessary) fear of a potential threat—to generate revenue from victims. In other words, Conficker served as a large-scale distributor for Waledac's wares.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

The Conficker-Waledac collaboration is an example of the networked and persistent threats that will likely become more prevalent. The threats are networked because they involve at least two enterprises collaborating with each other for illegal purposes, and they are persistent because the same attacks are launched from the same hosts over a long period of time—which means they can inflict greater damage.

Cisco security experts expect to see cyber criminals engaging in similar joint ventures in the coming months. In fact, they have located online advertisements that offer other criminals the ability to access existing botnets. In a recent online conversation with a botmaster, Cisco researchers learned that botnets can be sold off at a given price per "node" or infected system. As botnet creators become more capable of operating in stealth mode for longer periods of time, they will be able to earn more money before the botnets are detected and dismantled.

Depending on situation and opportunity, those who engage in online attacks have also been known to both collaborate with, and target, each other. One security researcher discovered that a major botmaster used an online forum to ask other criminals for help after his own botnet was hacked.



Наши тарифы

Азия*		12$
Микс*		22$
Европа*		40$
USA (США)**		140$
GB (Англия)**	WebMoney	220$
IT (Италия)**		150$
DE (Германия)**	Wire	170$
PL (Польша)**		150$
BR (Бразилия)**		150$
CA (Канада)**		200$
Остальные страны**		~250$(свяжитесь с нами

SOTONA
icq 539109
IN FRAUD WE TRUST

Country:	Rate in $ for 1000 installs:
US	130
UK	100
NL	25
FR	25
PL	18
IT	60
DE	25
ES	25
AU	50
GR	25
Other	18

As these advertisements indicate, online criminals see revenue opportunity in selling or renting out botnets.

Cause for Optimism: Organizations Collaborate to Shut Down Online Threats

As online criminals constantly adapt and refine their techniques for reaping illegal revenue, security professionals and individual computer users must become even more sophisticated in their own approaches to combating security threats. There are encouraging signs that aggressive "good guy" collaboration can succeed.

The Conficker Working Group is an excellent example. The group was founded in early 2009 as the Conficker botnet continued to spread, and now boasts more than 100 security organizations (including Cisco) as members. The group's website (www.confickerworkinggroup.org) publicizes news about recent Conficker infections, the latest patches to block the Conficker worm, and tests to check for infection. The collaborative efforts of Conficker members helped disrupt most of the worm's activities earlier this year (see page 5).

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Another positive example is the crippling of the Srizbi/Reactor Mailer botnet (see page 9). One Internet hosting company, McColo, hosted the Reactor Mailer command and control infrastructure that controlled Srizbi/Reactor Mailer. After an aggressive campaign documenting McColo's activities, the company's upstream Internet providers terminated McColo's service. Once McColo was shut down, worldwide spam volumes plummeted.

However, Srizbi/Reactor Mailer was able to shift its operations to a hosting company based in Estonia, and spam volumes originating from the botnet rose until Microsoft's Malicious Software Removal Tool (MSRT) disabled the majority of the bots. The availability of the MRST demonstrates how coordinated action can thwart such attacks for prolonged time frames.

In addition, there has been a greater focus from both government and international law enforcement on combating cybercrime and improving cybersecurity. Increased cooperation of law enforcement in the tracking, arresting, and extraditing of cyber criminals is anticipated —and 2009 has already seen some high-profile arrests (see "Prolific Scammers Caught and Indicted," page 5). Increased compliance requirements and improved vendor response are also expected.

Following a formal "60-Day Review" of cybersecurity in the United States, President Barack Obama announced that he will appoint a "cybersecurity coordinator" to oversee "a new comprehensive approach to securing America's digital infrastructure."[1] The Obama administration is expected to keep the spotlight on making improvements and embracing innovative thinking in both U.S. cybersecurity and technology policy.

According to the *Cyberspace Policy Review* report released by the White House in May 2009, the United States looks to "harness the full benefits of innovation to address cybersecurity concerns . . . [and] develop the policies, processes, people, and technology required to mitigate cybersecurity-related risks." The report also notes that the country "faces the dual challenge of maintaining an environment that promotes efficiency, innovation, economic prosperity, and free trade while also promoting safety, security, civil liberties, and privacy rights."

The United States is not alone in its desire to improve cybersecurity and prevent cyber criminals from achieving success. Because these are issues of global concern, it is no surprise that other countries are also increasing their efforts to address them.

For instance, the United Kingdom is currently conducting its own cybersecurity review. Results are expected to be published this summer along with an updated version of the country's National Security Strategy. It is anticipated that the United Kingdom will also create a cybersecurity coordinator-type post in its government. Meanwhile, Finland recently announced that it will establish, and activate by early 2011, a round-the-clock "cyberwar unit" responsible for protecting the country's data communications from both civilian and military cyber attacks.

> "We see many signs that criminals are mimicking the practices embraced by successful, legitimate businesses to reap revenue and grow their enterprises."
>
> TOM GILLIS,
> Vice President and General Manager,
> Cisco Security Products

[1] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," May 29, 2009, transcript released by The White House, Office of the Press Secretary, www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Online Security Risks and Trends

Malware: Conficker Combines Old and New Threats

The piece of malicious software that may have caused the most chaos in the first half of 2009 used an older method of attack that should have been easy to detect and avoid. Yet when the Conficker worm (also known as Downadup) began exploiting vulnerable devices in the last quarter of 2008, and continued to propagate through early 2009, it quickly spread to millions of computer systems, infecting tens of thousands of new machines daily. Experts agree that Conficker appears to be the largest worm infection since the SQL Slammer attack of 2003. Given that the Conficker worm was detected by security experts in October 2008, and that patches for the exploited vulnerability had been available since that time, this threat should have been easy to mitigate.

The Conficker worm actually has several variants, although Conficker.C (which includes .A and .B variants that downloaded the .C update) has been most successful at infecting large numbers of hosts. The worm infects computers by exploiting a vulnerability in the Microsoft Windows operating system (MS08-067/CVE-2008-4250). When executed, Conficker disables various Windows services such as Automatic Update and Security Center. It also blocks access to websites that would allow users to remove the infection. It then receives instructions through various communications channels, directing it to propagate, gather personal information, and download and install more malware onto victims' computers.

Given the amount of Windows vulnerabilities that require attention, this particular flaw may have been overlooked by IT professionals and individual computer users. In recent years, security has focused primarily on the web and email, and administrators may have neglected to install appropriate patches that would block Conficker's spread. About 150 countries have detected outbreaks of Conficker, with Brazil, China, and Russia showing the highest numbers of infected computer systems.

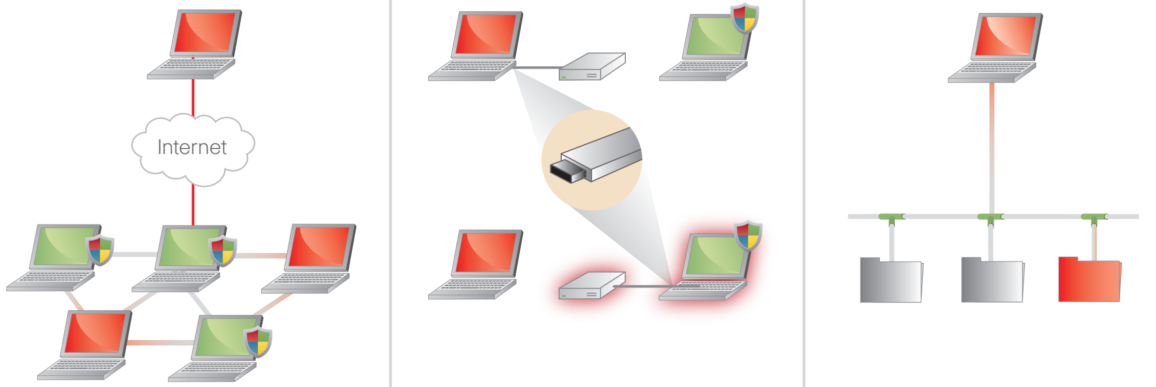
Although there may have been a dearth of attention focused on Conficker at the beginning stages of the infection, the spotlight grew as it became clear the worm's purpose was to build a massive botnet, perhaps the biggest ever. And when researchers realized that on April 1, 2009, the growing botnet would transition to a new method of communicating, media attention grew markedly. That, more than anything else, helped raise awareness of the Conficker problem, and spurred computer users to download the necessary patches. The Conficker botnet remains active, but rates of infection have slowed; as of early June 2009, it's estimated that about 3 million computers are still infected.

As April 1, 2009 (April Fool's Day in the United States) approached, security researchers were able to "dissect" the worm and piece together its plan of attack. On or about April 1, Conficker would begin generating thousands of Internet domain names and attempt to instruct some of them to download updated software. Although the botnet began generating 50,000 domain names per day compared to 500 before the April update, this method of communication was never actually put into place; one of the Conficker variants, an add-on module to Conficker.C, implemented peer-to-peer functionality instead.

The endgame for this activity appears to be the monetization of the botnet. In mid-April, the Conficker botnet was part of an outbreak of spam offering a free trial of software that would allow individuals to read supposedly private SMS messages. The malicious payload delivered via the fake SMS software was the Waledac botnet worm, which Conficker temporarily installed on infected hosts. It appears the creators of Conficker had allowed Waledac and some spyware to transport themselves via the large and well-established Conficker botnet. (Read more about Waledac on page 10.)

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Conficker: A Malware Triple Threat



Network–Based Infection

Conficker initially spread by exploiting the MS08-067/CVE-2008-4250 vulnerability. Any unpatched systems with ports 139 or 445 available were vulnerable.

Removable Storage–Based Infection

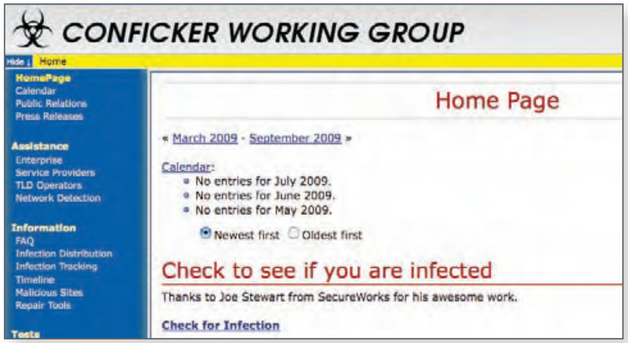
An infected computer can spread the infection, even to patched systems, if a removable storage device (for example, a USB drive) is shared between them.

Network Share–Based Infection

Conficker-infected hosts attempt to log into network shares. If successful, any other computers connecting to those network shares will become infected — even if they are already patched.

The rapid propagation of Conficker emphasizes the need for risk and threat management that intelligently determines that attacks can be sourced from anywhere in a network. Even an "old-school" vulnerability may be deployed by criminals—especially if they think corporate security experts and individual computer users are paying minimal attention to these types of threats.

A key takeaway from the Conficker experience is the value of collaboration in fighting back. The Conficker Working Group, composed of more than 100 organizations involved in technology and security (including Cisco), was formed in February 2009. ICANN, the organization that coordinates the Internet's naming systems and a member of the Conficker Working Group, was able to compile a list of the domain names Conficker was attempting to contact,



Home Page

« March 2009 · September 2009 »

Calendar:

- No entries for July 2009.
- No entries for June 2009.
- No entries for May 2009.

● Newest first ○ Oldest first

Check to see if you are infected

Thanks to Joe Stewart from SecureWorks for his awesome work.

Check for Infection

The Conficker Working Group website includes Conficker removal tools as well as a simple test to determine if a computer is infected.

Prolific Spammers Caught and Indicted

Thanks to collaborative efforts among legal authorities, security researchers, and other institutions, cyber criminals are being identified and prosecuted—and going to jail. In mid-2009, two brothers (Amir Ahmad Shah and Osmaan Ahmad Shah) were indicted by a U.S. federal grand jury for illegally harvesting students' email addresses, and bombarding them with spam messages offering everything from iPods to teeth-whitening services.

The brothers—one a current student at the University of Missouri, one a former student—used the spam to falsely portray themselves as representatives of the university. At the height of their operation in 2003, they were generating and delivering 1 million spam messages every hour to students at nearly 100 educational institutions across the United States.

Using information from the various affected schools, including the University of Missouri, Cisco researchers were able to chart the increases in spam traffic generated by the Shah brothers. The The Cisco SensorBase network, which collects live threat data from over 700,000 globally deployed security devices, provided researchers with a high-level view into the damage this spam was causing to computer networks. The data was shared with U.S. district attorneys, and eventually played a key role in building the government's successful case against the Shahs.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

thanks to data provided by security researchers tracking the worm. ICANN then passed this information to top-level domain operators, who could then block these domains. This coordinated effort went a long way toward blunting the impact of the worm.

When Conficker's creators realized the botnet's communications methods had been detected by security researchers, the scammers quickly shifted to a different approach. As criminals seek ways to monetize their activities and work to protect these revenue streams, they will fight back to prevent any tampering with their underground economy.

"Spamdexing": SEO for Online Criminals

As the media reported on the mayhem caused by Conficker, worried computer users took to Google and other search engines to locate patches to block the worm. Unfortunately, some of the most prominent first-page results—which users assumed to be trustworthy, since they were indexed ahead of all other results—were actually for sites hosting fake security software, and often, malware.

When prominent news events drive computer users to search engines—for instance, NCAA basketball tournaments in the United States, major holidays, or threats like Conficker—online criminals employ a technique called search engine poisoning, or "spamdexing," to push their fake websites to the top of search page results. Spamdexing involves overloading a webpage with relevant search terms or keywords so search engines will interpret the sites as good matches for the computer user's query—raising the ranking for the suspect pages.

Spamdexing isn't used solely by online criminals. Although search engine companies disapprove of the tactic, and supposedly employ methods to minimize the impact of spamdexing, many legitimate companies use this strategy to boost their own search rankings. And as discussed elsewhere in this report (see page 10), criminals have been quick to co-opt any practices deemed successful in the legitimate business world. In fact, they can use free online tools like Google Trends to discover the most popular search terms at any given time—and create malware-carrying fake websites accordingly.

User education in the form of security awareness training helps mitigate the threats posed by spamdexing, but enterprises can't assume employees will always make the correct choice about which websites to trust. For more thorough protection, businesses need security solutions that combine traditional URL filtering, reputation filtering, malware filtering, and data security.

Financial Information Targeted by DNS Poisoning

Domain Name System (DNS) cache poisoning has been a threat to online security for quite some time, but recent attacks indicate that criminals continue to use this method to obtain financial information—a key moneymaker for scammers. In April 2009, security researchers recorded what appears to be the first documented DNS cache poisoning attack on a financial institution—in this case, Brazil's Banco Bradesco. As with typical DNS-related attacks, the criminals redirected visitors from the bank's website to their own website, and offered up a fake login screen, presumably to steal login credentials.

There was hope in the security industry that DNS cache poisoning would become less prevalent once word got out about the Kaminsky DNS vulnerability (named after the security researcher who spotted a dangerous flaw in the Internet's DNS). Although exposure of this vulnerability led to development of effective patches, many DNS servers still remain unpatched.

Dynamic, real-time web reputation technology is the answer to the ongoing threat of DNS cache poisoning. By assessing the trustworthiness of all URLs that comprise a webpage—not simply using a URL blacklist or whitelist—attacks can be quickly detected and blocked.

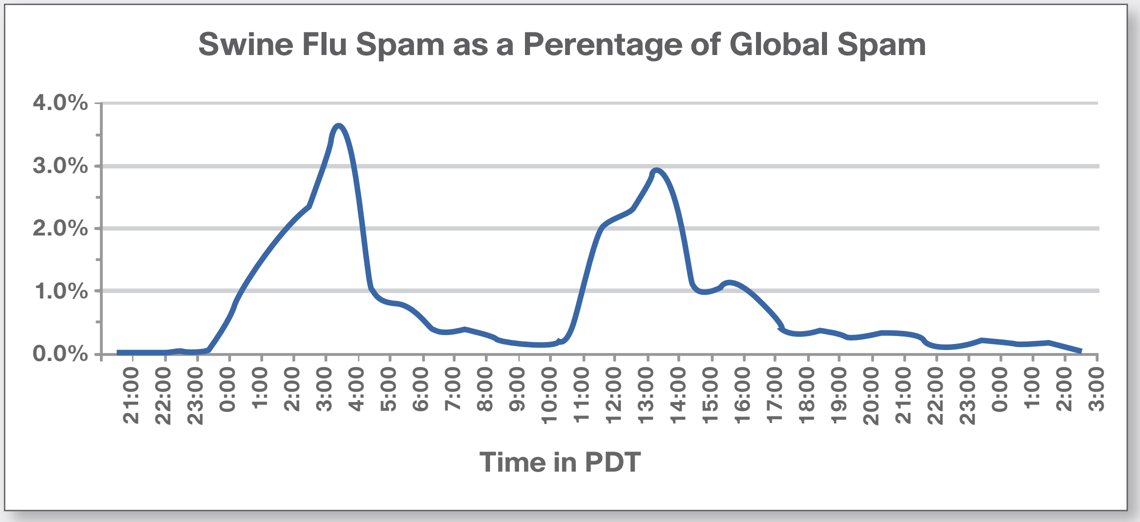
All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

User education in the form of security awareness training helps mitigate threats. But enterprises can't assume employees will always make the correct choice about which websites to trust.

Recent Social Engineering Spam Campaign: Swine Flu

The worldwide outbreak of H1N1 influenza (commonly referred to as "swine flu") that began in April 2009 quickly led to an outbreak of another kind—a barrage of spam emails using swine flu as the bait. In late April 2009, cyber criminals started sending spam messages with subject lines such as "US swine flu fears" and "Swine flu in Hollywood." Recipients who clicked through were rewarded with messages urging them to buy nonexistent swine flu preventive drugs, along with a link to various websites known to sell fake pharmaceutical products.

At the peak of the outbreak, swine flu-related spam messages comprised nearly 4 percent of global spam traffic. However, enterprise computer users with robust anti-spam solutions and web reputation filters probably saw very few of the messages because they were quickly blocked. Alert IT departments and computer users should assume that every time a major story like the swine flu outbreak hits the news media, spammers will seize the chance to launch an attack using these social engineering techniques.

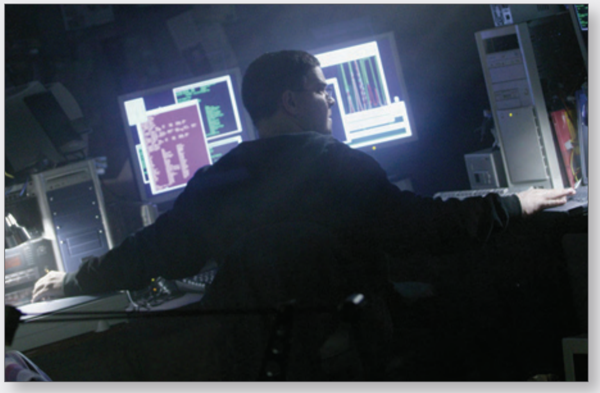


As swine flu dominated global news stories, cyber criminals took advantage of its popularity to send more spam. Given the perfect storm of high popularity and low prior knowledge, people turned to the Internet to learn more about H1N1 influenza. Cyber criminals seized the opportunity by sending billions of spam messages—accounting for up to 4 percent of global spam at its peak.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Conversations with a Botmaster

Why does someone go into the business of creating and running a botnet? Not for the glory, discovered Cisco researchers who ended up chatting with a botmaster—but for the money. The botmaster who offered up an insider's look at the world of running botnets pegged a typical botmaster's income at US$5,000 to US$10,000 a week. And today, this income potential only demands a minimal level of technical knowledge, along with a savvy sense of how to con computer users into falling for the right lure.



The online conversation with this particular botmaster took place after Cisco researchers detected and removed a botnet infection. The researchers had noticed a high level of Internet Relay Chat (IRC) traffic over the network on nonstandard ports—usually a good indicator of malicious activity.

One of the researchers, pretending to be a fellow botmaster, posted a polite opening query via IRC. When the botmaster responded, the researcher asked what the botnet would be used for. The botmaster replied that he planned to gain control of several thousand machines, and sell them off to online criminals for their own schemes for 10 to 25 cents per node, or bot. The botmaster said he had recently sold 10,000 infected machines for US$800.

The researcher asked the botmaster how he gained control of so many machines, expecting him to say he'd exploited a known vulnerability using a worm like Conficker (see page 4). But the answer was surprising: The botmaster had sent out thousands of pieces of spam via instant messaging applications, with messages along the lines of "Check out this cool software," and a link to the botnet malware. Even if only 1 percent of the recipients were careless enough to follow on the link, the botmaster gained control of enough machines to make the effort worthwhile.

The researcher then asked the botmaster why he sells bots instead of using them for spam or phishing networks. The botmaster replied that selling bots wasn't usually his goal, since earnings were modest. In this instance, he had sold off 10,000 machines because he needed money for antibiotics for his sick child—but the real money, he said, came from using the bots for phishing attacks, in which personal information, such as banking passwords, is stolen. When the researcher asked how much money could actually be made from phishing activities, the botmaster was evasive about his own income, but said "a guy he knew" was able to earn US$5,000 to US$10,000 a week solely through phishing activities.

Why did the botmaster—someone obviously skilled with technology—choose this type of work instead of seeking a legitimate IT position? The botmaster said that a criminal record and lack of a "decent education" prevented him from obtaining an above-board job. In this faltering economy, one has to wonder if even well-educated IT experts with no criminal record will resort to illegal activities, since jobs are so scarce.

The Cisco researchers were also struck by the fact that neither the botnet nor the method of attracting victims (instant-messaging applications) were overly complex. It is not necessary to understand code, nor is there a need to understand networking.

Given the fact that anyone with a moderate understanding of the technology can bring a botnet to life, the implications for enterprise security are sobering," said Jeff Shipley, Security Research and Operations Manager at Cisco. "Patching to prevent threats against known vulnerabilities is key, but security awareness training about safe online behavior is even more important."

Read the full-length "Infiltrating a Botnet" Cisco report at www.cisco.com/web/about/security/intelligence/bots.html.

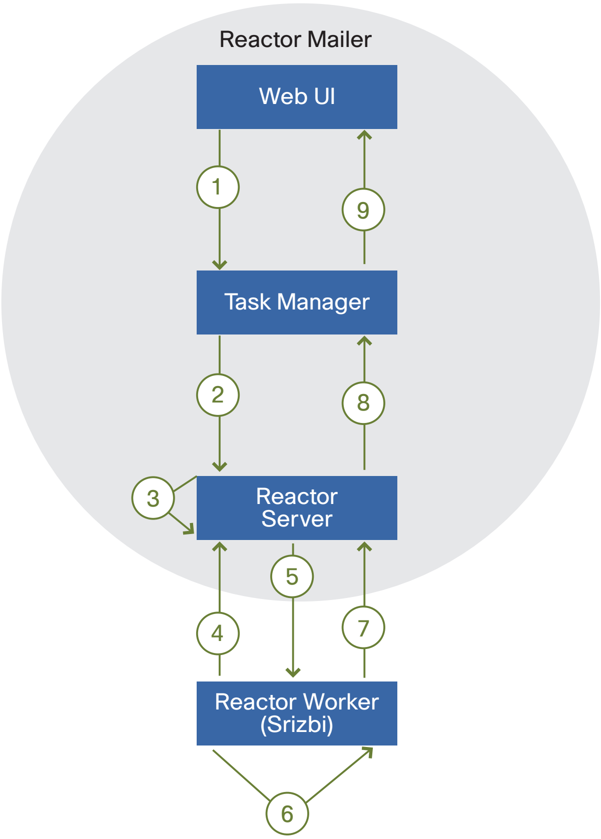
All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Botnets: The Rise—and Fall—of Srizbi/Reactor Mailer

In 2008, one of the biggest stories from the botnet world was Storm, which used innovative social engineering techniques to spread infection. As Storm's power waned, thanks to higher awareness and more effective threat-removal tools, the Srizbi/Reactor Mailer botnet took center stage, and, at its peak, dwarfed Storm in both size and output. By mid-2008, the Srizbi botnet had a stable population of 260,000 host computers and was responsible for the distribution of as much as 60 percent of the world's spam (a staggering 80 billion messages per day). Because it did not draw as much attention as Storm, Srizbi/Reactor Mailer operated unchecked for a longer period of time.

How did Srizbi achieve such success? Although it was initially distributed via "drive-by" downloads, Srizbi later used social engineering tactics to lure spam recipients into clicking through and downloading the malicious software. For instance, emails claimed the sender had a video file "where you look stupid." The unwitting recipient downloaded an executable file that turned the computer into a bot, or node, on the botnet.

This was standard operating procedure for botnet creators, but Srizbi/Reactor Mailer also had a secret weapon: a purpose-built "spam engine" that dramatically accelerated delivery of email messages generated by the individual nodes in the Srizbi botnets. Srizbi/Reactor Mailer was created by a spammer and sold to botnets using a software-as-a-service model—a good example of how online criminals are adopting best practices in business and technology to monetize their activity.



1 Create Task
2 Run Task
3 Create Atoms
4 Request Atom
5 Deliver Atom
6 Transmit 1000 Messages
7 Report Completed Atom
8 Aggregate Results
9 Report Results

The Srizbi/Reactor Mailer botnet was created as software-as-a-service—whereby spammers can create and deliver spam messages (tasks and atoms) through the botnet for a fee.

Srizbi/Reactor Mailer proved highly efficient at distributing spam because it eliminated a common bottleneck—that is, the transmission of spam, byte by byte, through a single data center. Srizbi/Reactor Mailer separated spam tasks into individual work units (called "atoms"), each with their own message templates, data files, and email lists. The atoms would then report back to the Reactor server when the work was completed. This process, combined with a large number of infected hosts, allowed Srizbi to deliver an unprecedented level of spam.

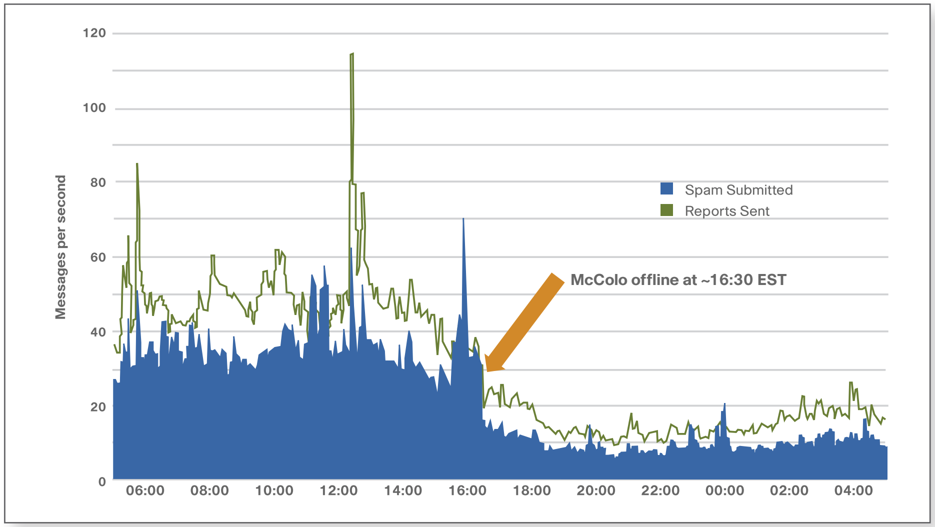
The Takedown of Srizbi/Reactor Mailer

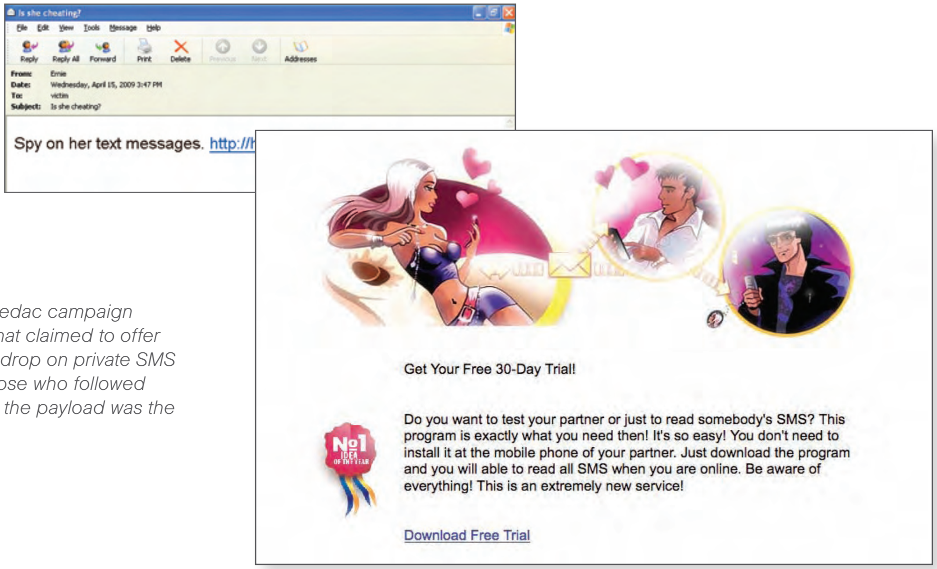
Srizbi/Reactor Mailer fell just as quickly as it became the world's leading distributor of spam. The first salvo against Srizbi occurred when McColo, the botnet's hosting provider, was shut down in November 2008. McColo had a reputation for hosting botnet command and control servers and online pharmacy payment processors. Srizbi/Reactor Mailer appeared to be McColo's largest single customer.

Srizbi/Reactor Mailer's major flaw was that its entire command and control infrastructure was hosted in the same data center on McColo. When McColo was taken down by its upstream providers, worldwide spam volumes immediately dropped by two-thirds, according to the Cisco SensorBase threat-tracking database. Within two weeks, Srizbi/Reactor Mailer was able to relocate its operations to Estonia, and by February 2009, it once again accounted for 60 percent of global spam volume.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Spam Volume Decline Due to McColo Shutdown




Is she cheating?
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses

From: Ernie
Date: Wednesday, April 15, 2009 3:47 PM
To: victim
Subject: Is she cheating?

Spy on her text messages. http://h

Get Your Free 30-Day Trial!

Do you want to test your partner or just to read somebody's SMS? This program is exactly what you need then! It's so easy! You don't need to install it at the mobile phone of your partner. Just download the program and you will able to read all SMS when you are online. Be aware of everything! This is an extremely new service!

Download Free Trial

A high-profile Waledac campaign delivered spam that claimed to offer software to eavesdrop on private SMS messages. For those who followed the enclosed link, the payload was the Waledac bot.

However, Microsoft dealt Srizbi/Reactor Mailer a crippling blow in February 2009. At that time, Microsoft added a signature for Srizbi to its Malicious Software Removal Tool (MSRT), eliminating most Srizbi infections in just a few weeks. Worldwide spam volumes plunged once again, this time to levels last seen in June 2007, according to SensorBase data. Srizbi has since mutated to a new botnet, Xarvester, in response.

Waledac: Storm 2.0

While Srizbi stole headlines in late 2008 and early 2009 as the spam powerhouse, the Storm botnet was morphing into Waledac—also called "Storm 2.0," because it came from the creators of Storm. Waledac began spreading its malware in earnest in early 2009, using emails referencing U.S. President-elect Barack Obama and the then-upcoming inauguration, as well as holiday-themed spam. Recipients were lured to a fake website and prompted to download an executable file containing the Waledac malware.

Waledac is notable for its use of fast-flux service networks, which both obscure the identity of web servers (often hosting illegal material such as malware and child abuse images), and make it harder to shut them down. The Storm botnet also used fast flux.

Waledac's most recent high-profile campaign, launched in April 2009, delivered spam that claimed to offer software that would allow users to eavesdrop on supposedly private SMS messages. As before, for the unfortunate recipients who followed the enclosed link, the payload was the Waledac bot.

The SMS spyware campaign is significant because the messages were sent through the Conficker botnet. This marked the first time that Conficker monetized itself by allowing Waledac to be downloaded via Conficker's hosts (read more about Conficker on page 4).

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Battling the Botnets

In response to coordinated and effective responses to major botnet threats, botmasters see value in trying to stay slightly under the radar. One method seen by Cisco and IronPort researchers is lower-volume but more frequent botnet attacks, which may allow criminals to avoid gaining attention while still yielding enough new bots. In a keynote address at the recent LEET '09 USENIX conference, Cisco IronPort senior security researcher Henry Stern noted that today's malware creators recognize the value of "boring" technologies and tactics that are slow to garner the attention of security experts—and therefore, have plenty of time to wreak havoc.

For instance, the Torpig botnet (which was "hijacked" for 10 days in early 2009 by computer science researchers at the University of California, Santa Barbara) has apparently been in operation for a few years now, stealing login credentials for hundreds of thousands of online bank accounts. The researchers were able to observe the botnet's activity as it accumulated an additional 180,000 infections and collected more than 70 gigabytes of data. Although the researchers gleaned valuable information from their brief takeover of Torpig, the botnet remains active.

There are also signs that botmasters are willing to collaborate—or at least sell or send each other their wares—to make money. The "SMS spying" Waledac attack emanating from Conficker-infected hosts is a good example. The Rustock botnet, another prolific source of spam, appears to be exploiting the same vulnerabilities used by variants of Conficker—a case of criminals "borrowing" strategies from their competitors.

As for how to battle botnets during future attacks: Locating and shutting down hosting providers like McColo had an immediate impact on spam traffic and computer infections, and the release of the MSRT had a slightly longer-term impact.

"These are not permanent solutions to the botnet problem, but they are very effective," said Patrick Peterson, Cisco Research Fellow and Chief Security Researcher. "Naturally, these tactics need to be deployed in tandem with network-based botnet mitigation and spam mitigation solutions."

Mobile Device Threats: Text Message Scams

Text message scams targeting users of handheld mobile devices, such as cell phones and smart phones, are becoming a common fraud tactic. At least two or three new campaigns have surfaced every week since the start of 2009. The spike in frequency can be attributed partly to the economic downturn, but it's also the massive—and still growing—size of the mobile device audience that is making this new frontier for fraud irresistible to criminals.

According to the International Telecommunications Union, there are more than 4.1 billion cell phone subscriptions worldwide. Cell phones have become the communications technology of choice for many individuals—particularly in developing countries. Meanwhile, the number of smart phones in use is expected to outpace cell phones in the near future. A criminal may cast a wide net with a text message scam—targeting, say, 1 million users at a time. But, even if that effort yields only 1000 victims, the scammers are likely to guarantee a decent return on their investment.

Many text message scams rely on social engineering tactics to dupe victims into handing over personal identification information or credit card numbers by purchasing worthless (or nonexistent) products or services or cashing in on a prize. For example, in a recent fake lottery scam, Qatar-based customers of telecommunications company Qtel were targeted by Pakistan-based fraudsters purporting to be from the Qtel headquarters in Dubai. Customers were contacted by either SMS or phone and asked to provide "verification details," such as bank account numbers, to collect a grand prize. Victims were also asked to purchase scratch cards worth QR500 (approximately US$135) and provide those numbers as "security" when they collected their fictitious prize.

More criminals are also taking advantage of the popularity of online banking, and are heading straight for victims' money by specifically targeting their ATM accounts and personal identification numbers (PINs) with well-designed and localized text message scams—and they're leaving virtually no trail.

Because more handheld mobile devices offer Internet capabilities and PC-like functionality, more customers are using them to conduct financial transactions while they are mobile. So, when they receive a text message from their bank alerting them to a problem with their account, they may not view such correspondence as suspect—especially because these campaigns are often very sophisticated. (Note: Generally, financial institutions will not email, call, or text consumers to obtain or confirm passwords, PINs, or other identifying information regarding their accounts.)

To make their schemes even more convincing, scammers will direct recipients of their SMS messages to call a telephone number. When victims follow through, they actually connect with what sounds very much like the real bank's automated customer service line. Through voice prompts, recipients are asked to verify their identity by providing their login ID or account number and PIN. Then, the user is "thanked" by the automated operator and informed their issue has been addressed. Meanwhile, the scammers are already logging into the victim's bank account and transferring money into other accounts.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Recently, smaller financial institutions have been the focus of many text message scams, likely because customers tend to have higher levels of trust and familiarity with local banks. The following are some examples of recent text message scams involving these types of financial institutions:

- Cell phone users in Fargo, North Dakota, received text messages claiming there was an issue with their account at First Community Credit Union and were directed to call an 888 number. Callers were connected to an automated system for the "General Protection Department" and asked to answer three questions to verify their identity and to disclose a credit card or bank account number.
- A "smishing" scam (a phishing attack using SMS) that targeted Buffalo Metropolitan Federal Credit Union customers in New York surfaced in early 2009. The text message included a link that, when accessed, took victims to a phishing site meant to look like a legitimate website associated with the bank. Once on the site, they were prompted to download a program—a Trojan that provided criminals with access to customers' personal information.
- Scammers sent text messages to an undetermined number of Verizon Wireless customers, telling them their BCT Federal Credit Union card had been deactivated and they needed to call a certain number to reactivate the card. Several customers responded and provided their 16-digit card numbers and PINs, according to the bank, which operates in New York and Pennsylvania. The scammers used the information to recreate cards, withdraw money at ATMs, and make purchases.

Not surprisingly, telemarketing scams involving cell phones are also on the rise, and mirror "traditional" landline schemes. For instance, scammers tell victims that their auto warranty has expired and convince them to purchase a worthless insurance policy. Or, hoping to cash in on individuals' hard luck during the recession, they offer to help consumers get out of credit card debt or pay off their mortgage.

Consumers can put their mobile phone number on the United States Federal Trade Commission's (FTC's) Do Not Call Registry, and both the FTC and the United States Federal Communications Commission, which regulates cell phones, have made it clear that telemarketers may not use automated dialers to call cell phone numbers. Of course, scammers ignore such warnings, and because so many cell phones and smart phones are in use today, law enforcement cannot keep pace with the number of complaints they receive about telemarketing and text message scams that target users of these devices.

U.S. Government: A New Administration, a New Focus on Cybersecurity

As a candidate for the U.S. presidency, Barack Obama made it clear that, if elected, his administration would "make cybersecurity the top priority that it should be in the 21st century"[2] and put particular focus on its role in both homeland security and the nation's overall technology policy. He emphasized that information infrastructure, critical infrastructure sectors, and consumer safety were of great importance for the country.

Shortly after his inauguration in January 2009, President Obama launched a "60-Day Review" of the nation's cybersecurity infrastructure. Completed in May, this broad review included government systems, critical infrastructure sector systems, and consumer systems—domestic and global. The "comprehensive, clean-slate review to assess U.S. policies and structures for cybersecurity"[3] was the Obama administration's first major step toward:

- Developing a comprehensive cybersecurity policy for the United States
- Positioning the White House to assume a leadership role in protecting the nation's information infrastructure
- Fostering global cooperation on cybercrime, best practices, and ensuring a safer networking environment

[2] Remarks made by Senator Barack Obama at the Summit on Confronting New Threats, University of Purdue, July 16, 2008. Text of speech available on the Council on Foreign Relations' website: www.cfr.org/publication/16807/barack_obamas_speech_at_the_university_of_purdue.html.

[3] "Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure," May 2009, www.whitehouse.gov.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Also in April 2009, President Obama appointed Aneesh Chopra, Secretary of Technology for the Commonwealth of Virginia, as the first U.S. Chief Technology Officer. This move underscored the new president's pledge to make cybersecurity and technology priority items for the United States. It also highlighted the administration's intention to help develop a more collaborative and highly interactive relationship between the government and citizens. (It is expected that part of this long-term plan will include the embedding of collaboration technologies into government systems.)

Following the 60-Day Review, the administration issued the *Cyberspace Policy Review* report, which includes key findings from the review and recommendations for improving the nation's cybersecurity. Those recommendations, including 10 near-term actions, were discussed by President Obama during a speech in the East Room of the White House on May 29, 2009. They include:

- A cybersecurity policy official (a "cybersecurity coordinator") responsible for organizing U.S. cybersecurity policies and activities will be appointed. Also, a strong National Security Council (NSC) directorate to coordinate interagency development of cybersecurity-related strategy and policy should be established. This directorate should be under the direction of the cybersecurity coordinator, who will represent both the NSC and the National Economic Council.
- An updated national strategy (for the president's approval) to secure U.S. information and communications infrastructure will be prepared. This strategy should include continued evaluation of the Comprehensive National Cybersecurity Initiative's (CNCI) activities and, where appropriate, build on its successes. (The CNCI, approved by President George W. Bush in 2008, is designed to reduce the vulnerability of federal computer networks and critical infrastructure and mitigate the effects of attacks against those networks.)
- Appropriate, interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process should be convened. In addition, coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the federal government should be formulated.
- A national public awareness and education campaign to promote cybersecurity should be initiated.
- U.S. government positions for an international cybersecurity policy framework should be developed, and the nation should strengthen its international partnerships, to create initiatives that address the full range of activities, policies and opportunities associated with cybersecurity.

According to the Cyberspace Policy Review, innovation should also be leveraged to address cybersecurity concerns. The U.S. government should work with the private sector to "define performance and security objectives for future infrastructure, linking research and development to infrastructure development and expanding coordination of government, industry, and academic research efforts."

While lacking the detailed action plans that no doubt are under development now, the Obama administration's 60-Day Review and *Cyberspace Policy Review* report represent outstanding leadership in improving U.S. cybersecurity. Simply having the president making direct comments on cybercrime creates far more attention and action within government. The report's focus on "leading from the top" and alignment of resources in the executive branch with access to the president will ensure the topic gets the attention it deserves. *The Cyberspace Policy* Review report also offers a level of transparency that was not available in the previous administration's CNCI program.

Although there will always be material the federal government cannot reveal to the public, sharing as much as possible will enable all government employees and industry to participate in the new administration's cybersecurity initiative appropriately. In addition, the emphasis on public/private partnerships—especially international cooperation—is an essential element in reversing cybercrime trends. The Internet is operated and managed by many private, global enterprises. Cooperation with all of them worldwide to address cybersecurity issues is essential.

Through this 60-Day Review process, the Obama administration has put in motion changes that will transform the structure of cybersecurity leadership in the United States. However, the president has emphasized that this more intense focus on improving the nation's cybersecurity will not create new burdens for the private sector, but opportunities. In his remarks on the results of the 60-Day Review, President Obama said, "Let me be very clear: My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity."

In addition, the president has requested that more than US$400 million be included in the federal budget to support cybersecurity spending for the Department of Homeland Security, to protect critical infrastructure and IT networks from hackers.[4] And as part of the recent federal stimulus package, the American Recovery and Reinvestment Act (ARRA) of 2009, President Obama asked that US$7.2 billion be allocated for new broadband spending to support various projects, such as bringing broadband to rural areas and creating a "broadband map" of the United States.

[4] "Obama's Budget Calls for Shifts in IT Spending," by J. Nicholas Hoover, *InformationWeek*, May 8, 2009.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Additionally, US$11 billion will go to support a smart energy grid project that will modernize the way electricity is distributed throughout the country by integrating computer technology to help balance supply and demand from various energy sources. Recent events underscore the need for updating critical infrastructure, such as the U.S. electrical grid, in the interest of national security. "We know that cyber intruders have probed our electrical grid, and that in other countries, cyber attacks have plunged entire cities into darkness," said President Obama in his May 29, 2009, speech on cybersecurity.

While no such disruption has been reported in the United States to date, the grid-probing incident does point to the need for enhanced monitoring and control over such vital services. One such strategy is the Cisco plan for a "smart grid" that not only secures both physical and cybersecurity of electrical grids, but also helps utility companies manage power supplies and energy consumption more efficiently.

The ARRA also provides approximately US$20 billion for healthcare information technology. The legislation aims for widespread adoption of the use of electronic health records (EHRs) within the next decade and requires the federal government to develop standards by 2010 for the nationwide electronic exchange and use of health information to improve patient care.

The President's Smart Phone "Addiction"

The U.S. presidential election in November 2008 ushered in a new generation of leadership in the country—one that is at home with technology. And the man at the top, President Barack Obama, is someone who (like so many other individuals around the world) has wrapped his life around his personal technology use.

Being asked to relinquish his smart phone, the center of his "on the go" productivity and connectivity, would be unthinkable, even for the highest office in the land. So, when President-elect Obama—perhaps the most high-profile member among the legion of worldwide "CrackBerry" addicts today—was informed he would likely have to give up his beloved BlackBerry in the interest of national security, he resisted and asked the National Security Agency (NSA) to find a solution.

This caused a stir, primarily because this was a new issue for the NSA to tackle for the Oval Office. Eventually, President Obama won: It has been reported that the president currently keeps in touch with a select group of family and friends with a BlackBerry 8830 and uses a General Dynamics Sectera Edge smart phone for confidential government business. The Sectera Edge is reportedly one of only two types of smart phones that are approved to access the highly classified Secret Internet Protocol Router Network (SIPRNet).

According to media reports, President Obama will likely shift back to BlackBerry-only use once the appropriate security software is installed on the BlackBerry 8830 by the NSA—a day that may come very soon. Top aides and, of course, First Lady Michelle Obama, are expected to be issued the same devices.[6]

[5] "Inside Obama's Classified Smartphone," by Sascha Segan, PCMag.com, January 23, 2009, www.pcmag.com/article2/0,2817,2339444,00.asp.

[6] "Obama's BlackBerry Getting Final Security Touches," by Roy Mark, eWeek.com, April 23, 2009, www.eweek.com/c/a/Mobile-and-Wireless/Obamas-BlackBerry-Getting-Final-Security-Touches-475999/, and "Obama to Ditch Sectera Edge for BlackBerry?" by Sascha Segan, PCMag.com, April 24, 2009, www.pcmag.com/article2/0,2817,2345908,00.asp.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Technology: An Engine of U.S. Growth for the Next "New Economy"

Aside from the increased emphasis on improving U.S. cybersecurity, the Obama administration has shown a strong interest in defining and refining the nation's technology policy. It is becoming increasingly clear that the president views technology as playing a vital role in the nation's overall economic recovery and defining America's place on the global stage in the next "new economy."

The Obama administration's actions during its first 100 days in office indicate that the president believes investing in the nation's technology in the short term—whether for improving national defense, healthcare, power transmission, or other areas—will pay long-term dividends for the country and its citizens. In a way, what will happen over the next few years is not unlike the national highway system construction supported by President Dwight D. Eisenhower in the 1950s that continues to benefit us today. Instead, the bridges and highways being built or improved include those that make up the nation's IT infrastructure.

Whether it is the priorities of economic recovery, health-care (and healthcare IT), climate change and moving to a low-carbon economy (smart grids, smart buildings, smart transportation, and travel substitution), and education (technologies and schools, distance learning, and collaboration), it is obvious the new administration views technology as an engine of U.S. competitiveness and growth.

Geopolitical: Twitter Users Are Broadcasting the Revolution

Twitter, the microblogging service whose popularity skyrocketed in the first half of 2009, has been playing a starring role in political uprisings and demonstrations around the world. Although microblogging is legal and currently low-risk in terms of online security, the lightning-fast speed at which social networking services like Twitter can spur mass action is worth noting.

In response to allegations of voting fraud during Communist Party elections in the country of Moldova, students and other individuals protested on the streets of Chisinau, the capital, and learned of upcoming demonstrations via Twitter and other social networking vehicles. The government had shut down SMS texting and television stations. On one particular day of protests in early April 2009, Twitter posts meant to generate support for demonstrations were being delivered at a furious rate—new posts would appear every few seconds.

The same tactic was used by protestors during the G20 economic summit in London in April 2009. Protestors not only used social networking services (frequently from their mobile devices) to assure heavy turnout at demonstrations, but they also traded messages about evading the police. Of course, because many social networking posts are public, authorities could visit the same service to locate protesters and learn about planned activities.

Social networking's ability to summon crowds is also evident in the rise of "flash mobs," where individuals gather in large crowds—sometimes for a serious purpose and sometimes just for fun—to conduct some action, and then quickly leave the scene of the demonstration. Alerts about impending flash mobs are usually spread via social networks like Twitter. In May 2009, flash mobs appeared at several European airports, including London's Heathrow, to protest airport expansions.

The power and reach of social networking to bring about societal change is fascinating to watch, but also somewhat sobering because these tools won't always be used by the "good guys." All types of political activities—demonstrations, coup attempts, and general unrest—can take place at a far more rapid pace than ever before, posing a greater risk of instability for emerging markets and governments.

Economic Instability and Online Security

As worldwide unemployment rises and the job market tightens, security watchers assume that online crime may also be on the upswing. Employees who have been laid off, particularly those with IT skills, may see no option but to turn to online scams or other criminal activity. A subset of disgruntled employees without jobs may also be tempted to earn money by targeting former employers through network attacks or the theft and sale of intellectual property. (See "Conversations with a Botmaster" on page 8 for insights on why individuals with IT talent might choose illegal work over a legitimate job.)

In May 2009, the *Financial Times* reported that fraud committed by employees against their own companies may be on the rise, owing to the weak economy. The newspaper cited statistics from "whistleblower" hotlines, showing an increase in tips about insider crime. And in April 2009, the Association of Certified Fraud Examiners, the world's largest anti-fraud organization, released its report, *Occupational Fraud: A Study of the Impact of an Economic Recession.* According to the report, 90 percent of surveyed fraud examiners said they expect to see a rise in fraud over the next 12 months.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Vulnerabilities

The Weak Links in Social Networking

Web 2.0, the name for the collection of technologies and applications that make the Internet more collaborative and interactive, helped create the revolution in social networking. However, these lightweight, easy-to-use technologies aren't usually robust enough to block attacks from online criminals. The open, simple communication structure of Web-2.0-based applications is also its key weakness: Scammers who can exploit weaknesses in social networking sites can reach millions of potential victims with a single click.

Users of social networks place an undue amount of trust in members of their friend or contact lists. Criminals rely on this assumption to engage in social engineering-based scams—that is, they prey on computer users' assumptions that individuals in their communities won't send them malware-laden messages. So when a known community member sends friends a message with a link, recipients are far more likely to click through—inadvertently downloading malware, or ending up at a malicious website.

With a worldwide membership of 200 million as of May 2009, the social networking site Facebook has become a popular target for phishing attacks. According to phishtank.com, a website devoted to tracking phishing activity, about three separate phishing attacks were launched against the site on a daily basis in March 2009.

Microblogging service Twitter has also been susceptible to worm attacks. In April 2009, worms identified as "Mikeyy" or "StalkDaily" were spread by scammers who hacked into Twitter accounts and replaced the users' legitimate status updates with a link to a supposed celebrity website, StalkDaily.com. Each Twitter user who saw what they believed to be a friend's update and clicked on this link would then infect their own Twitter accounts, and cause the malicious link to be sent to their entire network. The 17-year-old hacker who created the "Mikeyy" worm said he did so "out of boredom"—an exception to most of today's malware attacks, which are launched to make money.

These worms were able to exploit a cross-site scripting vulnerability on the Twitter website. The attack had the potential to be far more malicious than it was, because it could have infected users' computers with malware instead of simply changing their Twitter status updates. This worm attack, like others aimed at social networks, demonstrates the need for more robust protection mechanisms built into the networks themselves.

Mac OS: Online Criminals Move Beyond Windows

In one of Apple's well-known "Mac vs. PC" commercials, "PC" laments the fact that his Windows-based computer is prone to security threats, while "Mac" stands complacently by. The implication is that the Mac operating system (OS) is far less vulnerable to security threats than Windows—so Mac users are more protected against online criminals.

Today, there are signs that criminals want to debunk the widely held assumption that the Mac OS is less prone to online attacks. Criminals are not targeting Macs because they perceive them to be less secure than they used to be, but rather because they offer greater opportunity for profit than before. Gartner Inc. has predicted that Apple will double its share of the computer market in the United States and Western Europe by 2011.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

The first botnet that seems to be specifically aimed at Macs was identified by security researchers in mid-2009. A malicious file appears to have been placed in pirated copies of Apple's iWork software and Adobe Photoshop for the Mac OS. That malware infected the computers of users who downloaded the pirated software and turned the systems into nodes for the botnet. There are signs the botnet is being used to launch distributed denial of service (DDoS) attacks.

In short, while "Mac" in the Apple commercial may have a relaxed attitude toward his ability to ward off online scammers, businesses and individuals relying on Macs should not adopt a similarly laid-back stance. Much like forward-thinking businesspeople, online criminals look for markets to exploit.The popularity of Macs presents the chance for criminals to launch new attacks in more places and grow botnets with more infected computers. Security policies should be applied regardless of the operating system or device that is used to access and share corporate data—whether it's a Microsoft Windows or Mac system, Apple iPhone, Palm or BlackBerry, protection needs to reside in the network.

> According to a recent study, 45 percent of surveyed privacy and security professionals said they had purchased cloud computing services for their companies, and an additional 22 percent are considering such a purchase.

Cloud Computing: Protecting Data in the Cloud

According to a recent study from Deloitte & Touche and the Ponemon Institute, 45 percent of surveyed privacy and security professionals said they had purchased cloud computing services for their companies (for such key services as data storage, email, and financial applications), and an additional 22 percent are considering such a purchase.

However, for the most part, these same professionals have not established plans for managing the security risks associated with ceding so much valuable corporate data to a third party. The Deloitte/Ponemon Institute study also reported that 82.6 percent of surveyed businesses had no formal plans in place to protect data they were entrusting to cloud providers. And in a recent IDC survey of companies' views of cloud services, respondents indicated that security was the greatest cloud-computing challenge they faced.

The cost-savings potential of cloud computing solutions could make them alternative models for some business operations, especially in challenging economic times. However, positive attention about the benefits of cloud computing may overshadow the possible risks that the solutions pose. At worst, security experts imagine scenarios wherein a hacker is able to compromise a single cloud system and access information or gain control of networks for hundreds of companies at once.

Cloud computing is one of the factors behind "deperimiterization," or the blurring of the lines of defense between corporate networks and the outside world (including online criminals). As such, cloud computing requires greater scrutiny in terms of security.

Businesses may lag in their understanding of the security implications of cloud computing. Any enterprise using cloud solutions must ask service providers about the type of security levels and controls stated in their service-level agreements, where and how their data is physically and logically stored, and compliance and regulatory documentation for the countries over which cloud services may travel.

Productivity Applications: Targets of Zero-Day Exploits

Online criminals continue to seek ways to launch exploits that are less suspect than, say, malware-laden spam. Vulnerabilities in popular productivity applications—such as Microsoft Word and Excel, and Adobe Reader and Acrobat—may be ripe for attack by scammers for the same reason popular social networking applications have become attractive. Users of these productivity applications perceive them to be safe environments and therefore are more likely to open documents provided by attackers. Additionally, targeted attacks against unknown vulnerabilities—known as zero-day attacks—allow criminals to continue to hide vulnerabilities from software vendors, preventing software fixes from becoming quickly available.

In early 2009, Adobe identified buffer overflow vulnerabilities that could cause some of its programs to crash, and possibly allow a hacker to take control of the user's computer. The company made appropriate patches available within a few weeks. Security researchers

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

detected exploits related to this vulnerability, so it was apparent that criminals were intending to make use of it. In May 2009, there were additional announcements about vulnerabilities in Adobe products. A similar flaw was identified by researchers in the Excel spreadsheet program in February 2009, but only after hackers used the vulnerability to take control of computer systems at businesses and government offices in Asia.

Since these exploits are often delivered via emailed files (for instance, Word or Excel documents or Adobe PDFs) that are commonly used in business environments, the best defense is user education. In years past, computer users were advised to exercise caution about opening executable (.exe) files; they should learn to apply the same level of skepticism to common productivity files that are coming from unexpected sources, or that raise suspicion because of the nature of the email message.

Barring user education, organizations can protect themselves against these threats with network-level signature and reputation systems. In addition, security solutions that monitor content of email messages (not just attachments) identify trends that indicate threat outbreaks and block email messages accordingly.

Top Alerts: January–June 2009

Adobe Acrobat Products PDF File Buffer Overflow Vulnerability	http://tools.cisco.com/security/center/viewAlert.x?alertId=17665
Adobe Reader Function Buffer Overflow Vulnerability	http://tools.cisco.com/security/center/viewAlert.x?alertId=18088
Worm: Conficker	http://tools.cisco.com/security/center/viewAlert.x?alertId=17121
GhostNet Spy Network Infiltrating Government and Private Systems	http://tools.cisco.com/security/center/viewAlert.x?alertId=17938 http://tools.cisco.com/security/center/viewAlert.x?alertId=17924
Gumblar Malicious Code Manipulates Search Engine Results to Increase Advertising Revenue	http://tools.cisco.com/security/center/viewAlert.x?alertId=18286
Worm: Koobface	http://tools.cisco.com/security/center/viewAlert.x?alertId=17240
Microsoft Office Excel Invalid Object Arbitrary Code Execution Vulnerability	http://tools.cisco.com/security/center/viewAlert.x?alertId=17689
Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability	http://tools.cisco.com/security/center/viewAlert.x?alertId=17519
Microsoft Office PowerPoint Arbitrary Code Execution Vulnerability	http://tools.cisco.com/security/center/viewAlert.x?alertId=17966
Malware Distributors Employ Search Result Poisoning to Target Unsuspecting Users	http://tools.cisco.com/security/center/viewAlert.x?alertId=18034
Worm: Waledac	http://tools.cisco.com/security/center/viewAlert.x?alertId=17327

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Web 2.0 Security: Filtering Dangerous Content

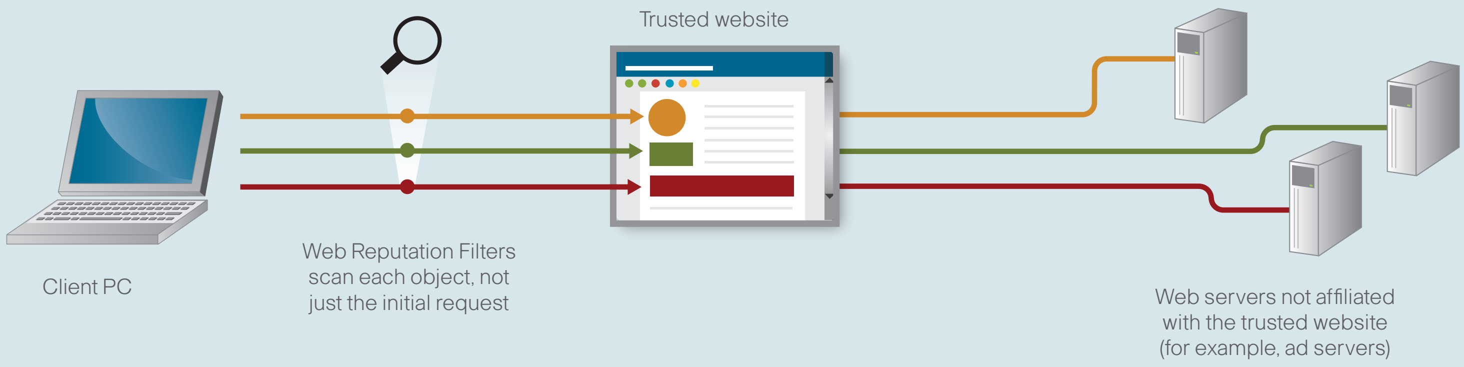
Dynamic Web 2.0 websites gather material from many sources, creating a richer experience for the website visitor—and a security headache. Online criminals intent on spreading malware now have many points of entry into websites, increasing their chances of success.

To the online visitor, who may only see the URL of a reputable site in the web browser, a malware attack can be impossible to spot. When a site is drawing its content from many third-party providers, there is no way to guarantee all of the component information is safe and free of malware.

Gumblar malware, which was racking up a number of hacked high-profile websites as of mid-2009, makes use of this Web 2.0 weakness. Gumblar begins its attack by exploiting legitimate websites through stolen FTP credentials and by leveraging vulnerable web applications through JavaScript. Visitors to these compromised websites are then exposed to malicious code that diverts search engine results to malware and phishing websites.

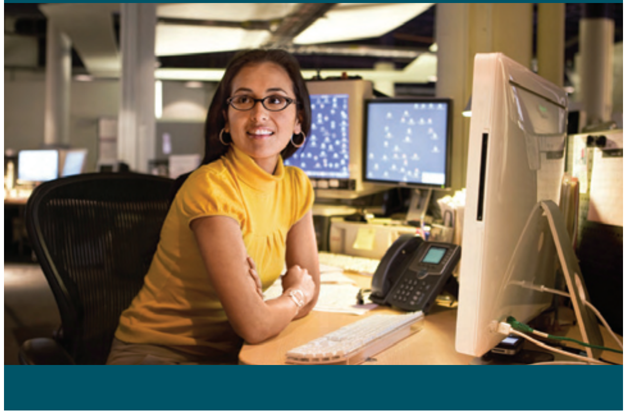
Preventing these kinds of attacks has become a key security requirement, as more and more websites pull content from third parties (a typical webpage can draw content from as many as 150 sources). URL filtering, one of the most common methods of blocking malicious content, is not effective; rather, a solution that examines every request for information made by a web browser as it loads content is necessary.

Protection For a Dynamic Web 2.0 World: Visibility Beyond the Initial Threat


Trusted website
Client PC
Web Reputation Filters scan each object, not just the initial request
Web servers not affiliated with the trusted website (for example, ad servers)

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Data Loss and Compliance



Data Loss

Identity Theft

The recession has created new moneymaking opportunities for at least one group of "entrepreneurs": identity thieves. As predicted in the *Cisco 2008 Annual Security Report*, spam, phishing, and text message scams are on the rise and growing in sophistication. Many of these campaigns are designed and deployed for the purpose of stealing identities to open new financial accounts or misuse existing ones.

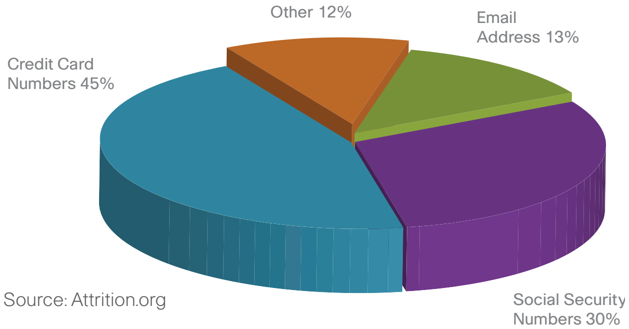
Of even greater concern is the role that "carding" (large-scale theft of credit card account numbers and other financial information) plays in funding terrorism and drug trafficking. According to a recent U.S. Department of Justice report, *Data Breaches: What the Underground World of Carding Reveals*, the "connection between identity theft—in particular as it relates to obtaining fraudulent identification documents—and terrorism is well established. In addition, links to drug traffickers engaging in identity theft for purposes of funding drug addictions is also well known."

The FTC reports that more than 9 million identities are stolen annually in the United States alone. Thirty-seven percent of complaints to the FTC deal with identity theft—by far the largest category of complaints the agency must field.

Researchers say that individuals ages 18 to 25 are at the highest risk for experiencing identity fraud today. This is primarily due to Generation Y's fondness for social networking. Identity thieves and hackers are trolling these sites regularly, searching for the keys to a user's identity—and finances. Users' profiles can provide a wealth of personal information—names, date of birth, hometown, and even phone numbers—that provide just enough detail for clever criminals to successfully commit fraud. Some have even gone so far as to contact a victim's friends and family members directly to request money.

Meanwhile, criminals continue to hack into personal email accounts to locate sensitive financial data or login information for websites. Or, they deploy social engineering techniques designed to lure unsuspecting victims to fake *and* legitimate websites, where they either willingly provide personal identification information, or unwittingly download keylogging malware that surreptitiously collects all the authentication details required for a criminal to gain access to their money. And with more botmasters looking to monetize their botnets, keylogging software is now being used to gather sensitive personal information from victims on a massive scale—stealthily.

Lost Record Types



Source: Attrition.org

Consistent with the greatest regulatory concerns, security professionals are most sensitive to data loss when credit card numbers, Social Security numbers, and private employee and customer records are lost.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Data Breaches

Data loss is a common problem for organizations, and it can be very costly: The Ponemon Institute estimates that in 2008, data breaches cost U.S. companies, on average, US$6.65 million, with the largest cost increase being lost business; this is an increase over 2007 at US$6.2 million. The Ponemon Institute also estimated the cost per record to be US$202.

According to the Privacy Rights Clearinghouse, which maintains a "Chronology of Data Breaches," 260 million personal records have been reported lost or stolen since January 2005—just in the United States. And the Identity Theft Resource Center (ITRC) says reported data breaches nearly doubled in 2008 from 2007. ITRC also says financial institutions were responsible for more than half of the 35 million personal records known to be lost or exposed during 2008.

The first major data breach reported in January 2009 involved a leading credit card processor. The company announced it had discovered—and had taken actions to resolve—a malware infection in its processing system that caused a 2008 breach, and that the incident may have been the result of a widespread global "cyber fraud" operation. The company processes cards for approximately 250,000 businesses in the United States, which means millions of credit and debit card transactions may have been compromised. The company reported a quarterly loss of more than US$2 million as a result of spending more than US$10 million in legal bills, fines from MasterCard and Visa, and administrative costs.

Insiders

Fraud, hacking, and identity theft by insiders are very real security threats, and they can be especially damaging for an organization because insiders know security weaknesses and how best to exploit them. Given the current economic downturn, in which many individuals have lost their jobs or become disgruntled—or set traps in advance to retaliate against an employer—insider threats can be expected to increase in the months ahead.

The Identity Theft Resource Center estimates that insiders were responsible for nearly a quarter of all known incidents involving financial institutions in 2008. That trend appears to be continuing in 2009. In April, a former employee at the Federal Reserve Bank of New York and his brother were arrested on suspicion of obtaining loans using stolen identities. According to the U.S. Federal Bureau of Investigation, one brother worked as an IT analyst for the bank and had access to sensitive employee information. Investigators found a USB flash drive attached to his computer with applications for US$73,000 in student loans using two stolen identities. They also found a fake driver's license with the photo of a bank employee who wasn't the individual identified in the license.

In a separate investigation, the U.S. Postal Inspection Service discovered that the fraudster's brother had opened a mailbox in New Jersey using a fake driver's license with a photo of a former or current employee of the Federal Reserve Bank of New York. He allegedly used the mailbox to receive documents for a boat loan obtained through the use of a stolen identity. He also is suspected of using a fake driver's license with another bank employee's photo in connection with the boat loan, and with using a bank employee's information for a phony income tax return.

Also in April 2009, a former employee of New York's Department of Taxation and Finance was arrested on charges that he illegally possessed sensitive personal data of thousands of New York residents and used the information to apply for and obtain credit cards. According to the office of State Attorney General Andrew Cuomo, the thief (who allegedly opened 90 fraudulent credit cards and other credit lines at more than 20 banks) had unpaid charges on accounts totaling more than US$200,000.

Among the fraudster's identity theft victims were a 4-year-old boy and at least four dead people, including his mother and sister. While employed for the Department of Taxation and Finance, he worked in a unit that scans identification documents, including birth certificates, submitted in connection with routine audits. Investigators found copies of more than 700 New York State tax forms; copies of more than 300 birth certificates and more than 1000 Social Security cards; and hundreds of pages of credit card statements, inquiry letters, applications, and cards in the criminal's and others' names.

In addition, as companies continue to look for ways to cut costs, they may increase their dependence on short-term staff, teleworkers, consultants, and third-party resources. Organizations will be wise to implement additional security policies regarding these resources and be particularly vigilant about the level and term of their access to sensitive data. One recent case: A disgruntled software engineer contractor who had worked for Fannie Mae for three years and had access to 4000 of the company's servers was indicted in January 2009 for allegedly planting a "logic bomb" in the mortgage lender's computer network. The embedded code was discovered by another engineer before it caused any damage, which would have been monumental, as the malicious script was designed to wipe out all data across Fannie Mae's network on January 31, 2009.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Web 2.0 Collaboration Quandaries and Mobile Device Dilemmas

In today's highly collaborative Web 2.0 environment, information is being shared between individuals inside and outside of an organization more often—and frequently in an insecure fashion. For example, according to a 2008 Cisco report titled, *The Challenge of Data Leakage for Businesses and Employees Around the World*, 44 percent of employees share work devices with others without supervision. Meanwhile, 18 percent share their passwords with coworkers.

Most organizations today have policies that provide clear guidelines about the devices and applications that employees are permitted to use while on the job. However, many workers find the rules constraining, and in the interest of conducting business more quickly and efficiently, ignore the rules that protect them and the organization. And until something costly or embarrassing happens, most users think nothing of the threat their carefree use of technology may pose to their employer.

Using technology that is not supported or approved by an organization can even compromise national security. In early 2009, Internet security firm Tiversa revealed that sometime during the summer of 2008, an unauthorized peer-to-peer file-sharing program installed on an employee's PC had led to a security breach in which blueprints "including planned engineering upgrades, avionic schematics, and computer network information" for the U.S. president's helicopter, Marine One, had been transferred to an IP address in Tehran, Iran. Tiversa reported that the address belongs to an "information concentrator," someone who searches peer-to-peer networks for sensitive information.

Mobile and handheld devices also create security headaches for organizations. Of course, with more of these devices on the work scene, there are more opportunities for employees to lose equipment containing sensitive data or login information. But there's more to the story: These devices, just like collaborative Web 2.0 applications, are playing a key role in stretching the traditional security perimeter.

Many workers—regardless of the policies their employers set—are using handheld devices, such as smart phones or netbooks, for both work and personal use. As more handheld devices are designed to offer PC-like functionality and a richer computing experience, users are expected to rely on their handheld devices even more to access business-critical information, including financial data and sales reports. Therefore, companies and their IT departments can expect mobile device security to remain a concern.

Collaborative applications and mobile devices can enhance workforce productivity and create cost savings. But businesses today face the challenge of balancing that productivity opportunity with the security risks it brings, and finding the right mix of policies and technologies to mitigate those risks. Going forward, companies will need to create policies and deploy solutions that protect sensitive data and prevent security threats, but that are also relevant for a Web 2.0 work environment where handheld devices are becoming the computing tools of choice.

Organizations must also take care when removing access rights after terminating any type of employee: A recent survey of laid-off workers conducted by the Ponemon Institute revealed that many companies are not doing enough to protect against data theft when they trim their workforce. Eighty-two percent of respondents said their employers did not perform an audit or review of documents before employees departed the company. Meanwhile, nearly a quarter of respondents said they still had access to the corporate network of their former employer after being laid off. According to the same study, more than 60 percent of those who purposefully took confidential data from a former employer also reported having an unfavorable view of the company.

Compliance

Around the world, there is an increase in legislation and industry initiatives around making data on networks more secure and informing those affected by data breaches. Today, there are many laws, regulations, and standards just in the United States related to data management. In fact, individual states are becoming much more aggressive about protecting their citizens from identity theft and other fraud; more than 40 states have already enacted data breach laws.

Nevada, for example, implemented a privacy law in 2008 that prohibits businesses from electronically transferring customers' personal data—such as first and last names, Social Security numbers, and bank account numbers—outside their organization, unless the data is encrypted. The law applies to data in motion and not "at rest."

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Massachusetts also passed a regulation in 2008 that requires all persons who own, license, store, or maintain personal information concerning the state's residents to protect that information from unauthorized access, disclosure, or misuse. Companies affected by the legislation must assess the risks to such information and develop written, comprehensive security programs that address them.

The Massachusetts regulation also requires affected entities "to the extent technically feasible [to implement] encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data to be transmitted wirelessly" as well as "all personal information stored on laptops or other portable devices."

Massachusetts' encryption requirement proved to be a major hurdle for compliance by the initial deadline of January 1, 2009, particularly for smaller organizations. Ultimately, the state extended the deadline for encryption of non-laptop devices twice, and it is now set for January 1, 2010. (The compliance date for encryption of laptops and data sent over public networks and wireless systems, however, is the new general compliance date of May 1, 2009.)

HIPAA Gets HITECH

On the healthcare compliance front, U.S. President Obama's 2009 American Recovery and Reinvestment Act (ARRA) stimulus package gave a boost to the Health Information Portability and Accountability Act (HIPAA): the Health Information Technology for Economic and Clinical Health Act (HITECH Act). This measure substantially raises the penalties for noncompliance for healthcare companies. It also contains regulations that expand the security and privacy provisions of HIPAA. More significantly, perhaps, it also generally extends some of those regulations to non-HIPAA-covered vendors of personal health records and their business partners.

The HITECH Act, like HIPAA, preempts any contrary state laws, but leaves intact any state laws and regulations that impose stricter requirements on the handling of patient information. Two examples of strict laws on the books: United States Senate Bill 541 (SB 541) and Assembly Bill 211 (AB 211), which California Governor Arnold Schwarzenegger signed in September 2008. These laws, which went into effect on January 1, 2009, are designed to improve patient privacy laws, address confidential health information leaks, and give the state the ability to assess and enforce fines for unauthorized disclosure of patient information.

AB 211 created a new State Office of Health Information Integrity (OHII) to oversee data issues and enforce statutes regarding confidentiality of healthcare data. OHII also is responsible for administering fines ranging from US$25,000 to US$250,000 on noncompliant entities. Meanwhile, SB 541 outlines the fine scale for healthcare organizations that commit data privacy and security violations that put patients at immediate risk of injury or death. The fines can run as high as US$50,000 for the first administrative penalty, up to US$75,000 for a subsequent administrative penalty, and up to US$100,000 for the third (and every subsequent) violation.

An organization that is covered by HIPAA and the HITECH Act must meet new minimum standards while continuing to monitor and comply with the growing number of laws governing patient information in every state in which the company operates. The HITECH Act's security breach notification requirements specify the timing, manner, and substance of any breach notification, among them:

- Notifying the Secretary of Health and Human Services "immediately" if the breach affects 500 or more individuals
- Notifying each individual whose unprotected health information is reasonably believed to have been accessed, acquired, or disclosed as a result of the security breach
- Providing notice to prominent media outlets in each state where the unsecured protected health information of 500 or more residents is reasonably believed to have been accessed, acquired or disclosed as a result of the breach
- Specifying in each notification to an individual a description of what happened, the types of information believed to have been accessed, and contact procedures for affected individuals to ask questions or learn more information

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

New “Red Flags” Rules

Because the concern around identity theft is escalating, it is driving more restrictive regulations both at the federal and state levels in the United States. This is creating additional burdens—in terms of money, time, and human resources—for businesses already working to be compliant with other existing laws, standards, or best practices, such as the industry-led Payment Card Industry Data Security Standard (PCI DSS), HIPAA, Gramm-Leach-Bliley Act (GLB), and Sarbanes-Oxley Act (SOX).

Of note are the new “Red Flags” Rules issued by the FTC, federal bank regulatory agencies, and the National Credit Union Administration. These rules—already delayed once before—were supposed to go into effect on May 1, 2009, but businesses now have until August 1, 2009, to develop their written programs. However, enforcement of the rules is scheduled to begin as planned on November 1, 2009. Examinations on financial institutions began in November 2008, and examinations for credit unions began April 2009.

In short, the rules require financial institutions and creditors to implement written identity theft programs for detecting, preventing, and mitigating instances of identity theft. Creditors that must comply with the rules are businesses that provide goods or services before billing, including industries such as telecommunications, utilities, and healthcare. The “red flags” to be monitored are patterns, practices, and specific activities that may indicate identity theft; for example, unusual account activity or attempted use of suspicious account application documents.

The program must also describe the appropriate responses that would mitigate the crime and detail a plan to update the program. (For more information on the “Red Flags” Rules, go to www.ftc.gov/opa/2008/10/redflags.shtm.)

Securing Data

More businesses are realizing their data is a vital asset, and are working to be more proactive about protecting it. As was recommended in the *Cisco 2008 Annual Security Report*, organizations must identify the data that they need to keep safe and place stronger controls where necessary. In short, they must let go of the view that they should try to protect everything, as that is an impossible task.

Companies also should strive to educate their employees and continually monitor email and web traffic to ensure sensitive information is not being shared inappropriately. Many organizations have implemented formal data loss prevention (DLP) programs to help secure their data—whether it is stored, in use, or moving around the network.

PricewaterhouseCoopers’ *2008 Global State of Information Security Study* reports that many organizations are also paying more attention to protecting sensitive data on mobile devices such as laptops—primary contributors to data loss because they are easily lost or stolen—as well as on databases, file shares, backup tapes, and removable media. Cisco advises its customers to deploy methods (preferably automated) to maintain the confidentiality of information on mobile devices, such as access controls, encryption, remote data removal, data association, redaction, truncation, or other methods that effectively render data unusable to unauthorized users.

Policies

Policies are a must-have for compliance audits. This is a primary focus for auditors—most compliance and industry best practices or regulations, such as HIPAA, the “Red Flags” Rules, PCI DSS 1.2, SOX, and GLB, require policies, which are thoroughly reviewed during audits.

Increasingly, companies are also realizing that these policies are important in the event that something does go wrong—such as a data breach that compromises customers’ credit card numbers—so they can show victims, attorneys and legal departments, shareholders, and law enforcement that they took clear steps to prevent such an event from happening.

While regulatory standards are designed to help protect user data, organizations should never view compliance as a security guarantee. In fact, as stated in the *Cisco 2008 Annual Security Report*, multiple security incidents in the previous year involved organizations considered to be “compliant.” However, compliance procedures are specific by design; they are intended to help organizations achieve only very specific objectives that mitigate only particular security risks.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Conclusion and Recommendations

Conclusion

Cybercrime, fueled by the global recession, is costing global businesses and individuals billions of dollars, according to recent industry estimates. It is a complicated world, with players big and small, organized and fringe, sharing a common desire to secure their own profits. Some players are just the guy or girl down the street—like the botmaster discovered and interviewed by Cisco researchers—who is content to scrape out enough to ensure a comfortable lifestyle. However, many other players are doing whatever possible—and more often now by pooling their resources and knowledge—to maximize their profits.

As predicted in the *Cisco 2008 Annual Security Report*, attacks are only going to become more sophisticated and targeted as we move through 2009. Social engineering is, and will remain, the technique of choice for criminals devoted to mastering the arts of trust-breaking and reputation-hijacking. To launch an attack, a social engineer might seize upon the hot topic of the day, such as swine flu or a major sports championship, or pose as someone (a friend or family member) or something (a local bank or a well-known company) to lure unsuspecting victims into handing over their personal information and ultimately, their identity and money.

Users, in droves, are also being convinced to install software that infects their systems and then harvests their personal information—or hijacks the machine so it will spam, infect, or con other users. Worse, users seeking protection from common cybercrime ultimately become victims anyway by turning to the Internet for help: They are duped into buying bogus anti-malware software to "clean up" their infected systems.

Meanwhile, there is increasing investment, focus, and success in malware used to infiltrate a computer and make it part of a botnet. Increasingly, botmasters are working to monetize their botnets, by renting them out, forming alliances, or blatantly exploiting each other—all at rapid speed. Many botmasters are borrowing the best practices and strategies of competitors, and even the real business world, to make their own attacks as high-impact as possible. These activities are all signs of the maturing online criminal economy, where tools and techniques can be easily assembled to quickly and quietly launch an attack affecting millions of people.

Security Community Making Strides

Although it's true that cybercrime is only becoming more pervasive, this year's positive news clearly illustrates the growing effectiveness of the means for fighting back. The unprecedented level of cooperation and participation by the security community and industry in response to the Conficker threat earlier this year marked an important turning point in the ongoing battle against cybercrime and fast-moving and far-reaching Internet security events.

The Conficker Working Group established for this strategic fight-back effort will no doubt serve as a model for the future. Conficker's impact—while significant and still playing out worldwide—has been dramatically reduced because multiple entities combined their knowledge, best practices, and technology to strategically, and as proactively as possible, hinder the spread of the worm.

It is obvious that those bent on committing cybercrime are taking advantage of the fact that many aspects of their targets (desktop operating systems, enterprise network infrastructure, DNS, hosting providers, and so on) are under the control of many different vendors, operators and entities. But the Conficker Working Group demonstrates that the industry can adapt and respond to a significant weakness rapidly and effectively. Thus, when the next major security threat emerges, the security community will know how to assemble and take action swiftly—together.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Through the Conficker experience, the security community also learned that although it may not be possible to clean up every infected computer in the world, it is possible to prevent infected computers from receiving new attack instructions, software binaries, and malware. Unfortunately, however, many of today's security threats are like the Hydra from Greek mythology: One head is cut off, and another grows back in its place. And as the underground economy grows and becomes easier for would-be criminals or simple opportunists to participate in, the Hydra becomes even more difficult to thwart.

One bright spot is that vulnerability and threat activity has been off to a slower start this year compared to 2008, according to Cisco research. This could indicate the security community is succeeding in making it more difficult for attacks to take root and grow.

There is even greater cause for optimism, as well: More cyber criminals—like the Shah brothers (see page 5)—are being identified and prosecuted. Many are going to jail. Security watchers are cautiously optimistic that future efforts to shut down online criminal activity will be increasingly supported by law enforcement. And President Obama has made it clear that improving cybersecurity is a front-burner issue for the United States, and the U.S. government is eager to work with the international community and the private sector to make the Internet safer for everyone.

2009 Threats and Vulnerabilities:
25 Percent Decrease From 2008 Activity Levels

Month	New Alerts	Updated Alerts	2009 Total	2008 Total
January	148	392	540	630
February	227	249	476	695
March	222	335	557	659
April	164	206	370	639
May	218	175	393	528
Totals	**979**	**1357**	**2336**	**3151**

Trends to Watch

Spam to Return to Record High Levels

Even actions that produce dramatic results provide only short-term relief, as has been the case with the takedown of Srizbi/Reactor Mailer. When hosting company McColo was shut down by its own Internet providers, worldwide spam volumes dropped dramatically and immediately. But it didn't last. Ever since the botnet's operators got back in the game with an Estonia-based hosting company, spam volumes have been climbing.

In addition, following the "noise" that helped to expose Conficker last year, botmasters have been working harder to conceal their activities for as long as possible so they can quietly grow their botnets to desired size. Thus, there has been a rise in lower-volume and more frequent botnet attacks recently.

In the months ahead, expect spam volumes to continue to rise to record levels. In May 2009, increases as high as pre-McColo levels were reported. In a 24-hour period around the U.S. Memorial Day holiday (May 25, 2009), just over 249 billion spam messages were sent—the third-highest volume day ever.

More Attacks on Legitimate Websites

Compromising legitimate websites for the purpose of propagating malware remains a popular and highly effective technique. Recent Cisco data shows that exploited websites are responsible for nearly 90 percent of all web-based threats.

Users expect websites from reputable organizations that they know or conduct business with to be safe, and therefore, are not likely to have their guard up when visiting these sites. Infecting legitimate websites also allows for precision targeting of certain groups, such as sports fans or students—an approach that has been very lucrative for cyber criminals. (And removes a great deal of their legwork.) Criminals are expected to maintain their aggressive targeting of legitimate websites, especially to distribute malware for creating botnets.

Social Networking Attacks to Continue

Cyber criminals go where the users are, which means social networking sites are becoming more popular haunts for attackers. In particular, identity thieves are finding great success on these sites, which can provide them with just enough information about a user to take advantage of that person, as well as their friends and family.

Criminals prey on a user's trust in their online community, and on their assumption that the people, companies, and organizations they interact with do not pose a threat to their security. This is why a user is likely to click through a link or download content that was sent to them by a trusted source, and in the process, inadvertently download malware or end up on a fraudulent or malicious website.

Worms have also been a problem for many popular social networking sites recently—and until these sites start featuring more robust protection that is built into the network, expect social networking communities to remain favorite hunting fields for many cyber criminals.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Recommendations

Security must move at the speed of crime. Organizations and users must not wait to patch their operating systems and applications. The list of vulnerabilities grows every day, as does the number of new applications (and versions of existing applications). Meanwhile, the complexity of attacks is increasing. Thus, businesses and users have no choice but to become more agile in deploying countermeasures and working with appropriate parties to respond to attacks.

In addition, security solutions need to be built to react rapidly. Anti-spam systems have become the blueprint for this model. For years now, new attacks have been developed and new techniques have been deployed to meet those threats effectively. All threats are heading in this direction and solutions must do the same.

History shows that many attacks and threats use the same vectors to exploit a vulnerability or compromise victims. Understanding the "anatomy" of an attack, and using multiple solutions and techniques that complement one another to prevent the threat from moving to the next phase, will help to disrupt and prevent the resulting infection quickly.

User education and security awareness training are critical. As was recommended in the *Cisco 2008 Annual Security Report*, employees should be expected to play a vital role in safeguarding their own online identity and understanding the risks that go along with their use of technology. Particularly, today's users must be educated as to how their growing reliance—and affinity for—Web 2.0 collaborative tools and applications and mobile devices that are not approved or supported by the enterprise pose significant security risks. Ongoing user education on security policies, technologies, and online threats, as well as clear guidance for meeting compliance measures, are essential.

Keep an eye on "old problems" while being vigilant about new risks. Unpatched or forgotten machines are those that will be infected first, giving attackers an "agent behind enemy lines" that can conduct inside-the-firewall attacks. Organizations must remember that a risk is a risk, and as criminals become more sophisticated and bold in their approaches, they will leverage an arsenal of techniques to carry out their attacks—even if the probability of any particular one being successful is low or remote.

Never underestimate the insider threat. The global recession has caused many individuals to lose their jobs—or face the prospect that they could be in the unemployment line soon. Meanwhile, employees who are spared layoffs may become disgruntled due to increasing workloads—and little or no relief or extra compensation for their stepped-up efforts or loyalty to their employer. As a result, insider threats will be of increasing concern for organizations in the months ahead. Insiders not only could be current or former employees, but contractors or other third parties. Insiders pose a very serious threat, as they know how to exploit an organization's weaknesses, security policies, and technologies to steal data, intellectual property, or money—or simply, disrupt operations.

The importance of strong (and realistic) policies for protecting sensitive data. Today's organizations need to create progressive policies that encompass anti-malware, acceptable use policies, and data loss prevention, and that are designed to help ensure regulatory compliance.

IT must work directly with management and employees to create and implement relevant, flexible, user-friendly policies that can be practiced and enforced throughout all levels of the organization.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

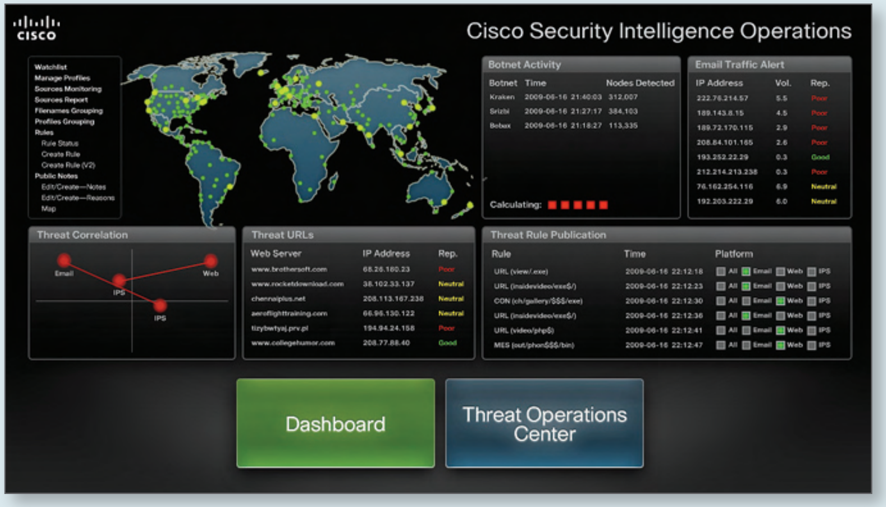
Cisco Security Intelligence Operations

Cisco Security Intelligence Operations (SIO) is an advanced security infrastructure that enables the highest level of security and threat detection and prevention for Cisco customers. With a team of global research engineers, sophisticated security intelligence, and automated update systems, Cisco SIO allows customers to embrace new technologies—securely—so they can collaborate with confidence.

Point defenses that meet individual security threats or protect individual products do not provide sufficient security in an environment where blended, cross-protocol, and cross-vendor vulnerability threats are increasingly the norm. Instead, integrated security management, real-time reputation assessment, and a layered, multipoint approach are required: a sophisticated, security ecosystem that provides a global view across various potential attack vectors.

Cisco SIO relies on tightly integrated data derived from multiple Cisco divisions and devices to assess and correlate Internet threats and vulnerabilities continuously. As threats continue to evolve, Cisco SIO will enhance the ability to identify global threat activities and trends, and provide expert analysis and services to help protect users from these threats.

Cisco is committed to providing complete security solutions that are integrated, timely, comprehensive, and effective—enabling holistic security for organizations worldwide. With Cisco, organizations can save time researching threats and vulnerabilities, and focus more on taking a proactive approach to security.



Botnet Activity

Botnet	Time	Nodes Detected
Kraken	2009-06-16 21:40:03	312,007
Srizbi	2009-06-16 21:27:17	384,103
Bobax	2009-06-16 21:18:27	113,335

Calculating: ■■■■■

Email Traffic Alert

IP Address	Vol.	Rep.
222.76.214.57	5.5	Poor
189.143.8.15	4.5	Poor
189.72.170.115	2.9	Poor
208.84.101.165	2.6	Poor
193.252.22.29	0.3	Good
212.214.213.238	0.3	Poor
76.162.254.116	6.9	Neutral
192.203.222.29	6.0	Neutral

Threat URLs

Web Server	IP Address	Rep.
www.brothersoft.com	68.26.180.23	Poor
www.rocketdownload.com	38.102.33.137	Neutral
chennaiplus.net	208.113.167.238	Neutral
aeroflighttraining.com	66.96.130.122	Neutral
tizybwtyaj.prv.pl	194.94.24.158	Poor
www.collegehumor.com	208.77.88.40	Good

Threat Rule Publication

Rule	Time	Platform
URL (view/.exe)	2009-06-16 22:12:18	☐ All ☑ Email ☐ Web ☐ IPS
URL (insidevideo/exe$/)	2009-06-16 22:12:23	☐ All ☑ Email ☐ Web ☐ IPS
CON (ch/gallery/$$$/exe)	2009-06-16 22:12:30	☐ All ☐ Email ☑ Web ☐ IPS
URL (insidevideo/exe$/)	2009-06-16 22:12:36	☐ All ☑ Email ☐ Web ☐ IPS
URL (video/php$)	2009-06-16 22:12:41	☐ All ☐ Email ☑ Web ☐ IPS
MES (out/phon$$$/bin)	2009-06-16 22:12:47	☐ All ☐ Email ☑ Web ☐ IPS

Cisco Security Intelligence Operations provides the highest level of threat correlation—enabling users to collaborate with confidence.

All contents are Copyright © 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Report available for download at

www.cisco.com/go/securityreport

For More Information

Cisco Security Intelligence Operations
www.cisco.com/security

Cisco Security Blog
blogs.cisco.com/security

SenderBase
www.senderbase.org

Cisco Security Solutions
www.cisco.com/go/securitysolutions
www.cisco.com/go/ros

Cisco Security Products
www.cisco.com/go/security
www.cisco.com/go/intellishield
www.cisco.com/go/ips
www.ironport.com

Cisco Corporate Security Programs Organization
www.cisco.com/go/cspo

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at **www.cisco.com/go/offices**.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

S. 773 – Cybersecurity Act of 2009
SUMMARY

Cybersecurity Act of 2009 - Directs the President to establish or designate a Cybersecurity Advisory Panel to advise the President. Defines "cyber" as: (1) any process, program, or protocol relating to the use of the Internet or an intranet, automatic data processing or transmission, or telecommunication via the Internet or an intranet; and (2) any matter relating to, or involving the use of, computers or computer networks. Directs the Secretary of Commerce to: (1) develop and implement a system to provide cybersecurity status and vulnerability information regarding all federal information systems and networks managed by the Department of Commerce; and (2) provide financial assistance for the creation and support of Regional Cybersecurity Centers for small and medium sized U.S. businesses. Requires the National Institute of Standards and Technology (NIST) to establish cybersecurity standards for all federal government, government contractor, or grantee critical infrastructure information systems and networks. Makes NIST responsible for U.S. representation in all international cybersecurity standards development.

Directs the Secretary to develop or coordinate a national licensing, certification, and recertification program for cybersecurity professionals and makes it unlawful to provide certain cybersecurity services without being licensed and certified. Requires Advisory Panel approval for renewal or modification of a contract related to the operation of the Internet Assigned Numbers Authority. Requires development of a strategy to implement a secure domain name addressing system. Requires the National Science Foundation (NSF) to support specified types of research and to establish a program of grants to higher education institutions to establish cybersecurity testbeds. Amends the Cybersecurity Research and Development Act to expand the purposes of an existing program of computer and network security research grants. Requires the NSF to establish a Federal Cyber Scholarship-for-Service program. Requires NIST to establish cybersecurity competitions and challenges to recruit talented individuals for the federal information technology workforce and stimulate innovation. Requires the Department of Commerce to serve as the clearinghouse of cybersecurity threat and vulnerability information. Grants the Secretary access to all relevant data concerning such networks notwithstanding any law or policy restricting access. Directs the President to: (1) develop and implement a comprehensive national cybersecurity strategy; (2) on a quadrennial basis, complete a review of the cyber posture of the United States; and (3) work with representatives of foreign governments to develop norms, organizations, and other cooperative activities for international engagement to improve cybersecurity. Requires the Director of National Intelligence and the Secretary of Commerce to submit to Congress an annual report on cybersecurity threats to and vulnerabilities of critical national information, communication, and data network infrastructure. Establishes a Secure Products and Services Acquisitions Board to review and approve high value products and services acquisition and establish validation standards for software to be acquired by the federal government.

National Cyber Alert System[1]
Cyber Security Tip ST05-019

Preventing and Responding to Identity Theft

Identity theft, or identity fraud, is a crime that can have substantial financial and emotional consequences. Take precautions with personal information; and if you become a victim, act immediately to minimize the damage.

Is identity theft just a problem for people who submit information online?

You can be a victim of identity theft even if you never use a computer. Malicious people may be able to obtain personal information (such as credit card numbers, phone numbers, account numbers, and addresses) by stealing your wallet, overhearing a phone conversation, rummaging through your trash (a practice known as dumpster diving), or picking up a receipt at a restaurant that has your account number on it. If a thief has enough information, he or she may be able to impersonate you to purchase items, open new accounts, or apply for loans.

The internet has made it easier for thieves to obtain personal and financial data. Most companies and other institutions store information about their clients in databases; if a thief can access that database, he or she can obtain information about many people at once rather than focus on one person at a time. The internet has also made it easier for thieves to sell or trade the information, making it more difficult for law enforcement to identify and apprehend the criminals.

How are victims of online identity theft chosen?

Identity theft is usually a crime of opportunity, so you may be victimized simply because your information is available. Thieves may target customers of certain companies for a variety of reasons; for example, a company database is easily accessible, the demographics of the customers are appealing, or there is a market for specific information. If your information is stored in a database that is compromised, you may become a victim of identity theft.

Are there ways to avoid being a victim?

Unfortunately, there is no way to guarantee that you will not be a victim of online identity theft. However, there are ways to minimize your risk:

Do business with reputable companies - Before providing any personal or financial information, make sure that you are interacting with a reputable, established company. Some attackers may try to trick you by creating malicious web sites that appear to be legitimate, so you should verify the legitimacy before supplying any information (see Avoiding Social Engineering and Phishing Attacks and Understanding Web Site Certificates for more information).

Take advantage of security features - Passwords and other security features add layers of protection if used appropriately (see Choosing and Protecting Passwords and Supplementing Passwords for more information).

Check privacy policies - Take precautions when providing information, and make sure to check published privacy policies to see how a company will use or distribute your information (see Protecting Your Privacy and How Anonymous Are You? for more information). Many companies allow customers to request that their information not be shared with other companies; you should be able to locate the details in your account literature or by contacting the company directly.

[1] Excerpted from United States Computer Emergency Readiness Team (US-CERT) http://www.us-cert.gov/cas/tips/ST05-019.html

Be careful what information you publicize - Attackers may be able to piece together information from a variety of sources. Avoid posting personal data in public forums (see Guidelines for Publishing Information Online for more information).

Use and maintain anti-virus software and a firewall - Protect yourself against viruses and Trojan horses that may steal or modify the data on your own computer and leave you vulnerable by using anti-virus software and a firewall (see Understanding Anti-Virus Software and Understanding Firewalls for more information). Make sure to keep your virus definitions up to date.

Be aware of your account activity - Pay attention to your statements, and check your credit report yearly. You are entitled to a free copy of your credit report from each of the main credit reporting companies once every twelve months (see AnnualCreditReport.com for more information).

How do you know if your identity has been stolen?
Companies have different policies for notifying customers when they discover that someone has accessed a customer database. However, you should be aware of changes in your normal account activity. The following are examples of changes that could indicate that someone has accessed your information:

unusual or unexplainable charges on your bills
phone calls or bills for accounts, products, or services that you do not have
failure to receive regular bills or mail
new, strange accounts appearing on your credit report
unexpected denial of your credit card

What can you do if you think, or know, that your identity has been stolen?
Recovering from identity theft can be a long, stressful, and potentially costly process. Many credit card companies have adopted policies that try to minimize the amount of money you are liable for, but the implications can extend beyond your existing accounts. To minimize the extent of the damage, take action as soon as possible:

Contact companies, including banks, where you have accounts - Inform the companies where you have accounts that someone may be using your identity, and find out if there have been any unauthorized transactions. Close accounts so that future charges are denied. In addition to calling the company, send a letter so there is a record of the problem.

Contact the main credit reporting companies (Equifax, Experian, TransUnion) - Check your credit report to see if there has been unexpected or unauthorized activity. Have a fraud alerts placed on your credit reports to prevent new accounts being opened without verification.

File a report - File a report with the local police so there is an official record of the incident. You can also file a complaint with the Federal Trade Commission.

Consider other information that may be at risk - Depending what information was stolen, you may need to contact other agencies; for example, if a thief has access to your Social Security number, contact the Social Security Administration. You should also contact the Department of Motor Vehicles if your driver's license or car registration have been stolen.
The following sites offer additional information and guidance for recovering from identity theft:

Federal Trade Commission - http://www.ftc.gov/bcp/edu/microsites/idtheft/
United States Department of Justice - http://www.usdoj.gov/criminal/fraud/websites/idtheft.html
Social Security Administration - http://www.ssa.gov/pubs/idtheft.htm

Identity Theft Statutes and Criminal Penalties[1]
(examples from local jurisdictions)

District of Columbia	22-3227.01 to 3227.08	Identity theft in the first degree	Any person convicted of identity theft shall be fined not more than (1) $10,000, (2) three times the value of the property obtained, or (3) three times the amount of the financial injury, whichever is greatest, or imprisoned for not more than 10 years, or both, if the property obtained or the amount of the financial injury is $250 or more. Any person convicted of identity theft shall be fined not more than $1,000 or imprisoned for not more than 180 days, or both, if the value of the property obtained or the amount of the financial injury, whichever is greater, is less than $250.
		Identity theft in the second degree	Any person who commits the offense of identity theft against an individual who is 65 years of age or older, at the time of the offense, may be punished by a fine of up to 1 1/2 times the maximum fine otherwise authorized for the offense and may be imprisoned for a term of up to 1 1/2 times the maximum term of imprisonment otherwise authorized for the offense, or both.
		Enhanced penalty	When a person is convicted of identity theft, the court may, in addition to any other applicable penalty, order restitution for the full amount of financial injury.
		Restitution	
Maryland	Criminal Law §8-301 to §8-305	Identity fraud	Misdemeanor where the benefit, credit, good, service, or other thing of value has a value of less than $500; punishable by imprisonment not to exceed 18 months or a fine not exceeding $5,000, or both Felony where the benefit, credit, good, service, or other thing of value has a value of $500 or greater; punishable by imprisonment not to exceed five years or a fine not exceeding $25,000, or both Felony; punishable by imprisonment not to exceed five years or a fine not exceeding $25,000, or both
		Intent to manufacture, distribute or dispense	Misdemeanor; and on conviction is subject to imprisonment not exceeding 18 months or a fine not exceeding $5,000 or both

[1] Excerpted from the National Conference of State Legislatures website, http://www.ncsl.org/default.aspx?tabid=12538

		identities Assuming identity of another/Representation without authorization Restitution Identity theft passport	In addition to restitution under Title 11, Subtitle 6 of the Criminal Procedure Article, a court may order a person who pleads guilty or nolo contendere or who is found guilty under this section to make restitution to the victim for reasonable costs, including reasonable attorney's fees, incurred: (1) for clearing the victim's credit history or credit rating; and (2) in connection with a civil or administrative proceeding to satisfy a debt, lien, judgment, or other obligation of the victim that arose because of the violation.
Virginia	18.2-152.5:1	Using a computer to gather identifying information; penalties	Any person who violates this section is guilty of a Class 6 felony. Any person who violates this section and sells or distributes such information to another is guilty of a Class 5 felony. Any person who violates this section and uses such information in the commission of another crime is guilty of a Class 5 felony. Class 1 misdemeanor Any violation resulting in financial loss of greater than $200 shall be punishable as a Class 6 felony.
	18.2-186.3	Identity theft; penalty; restitution; victim assistance	Any second or subsequent conviction shall be punishable as a Class 6 felony. Any violation of subsection B where five or more persons' identifying information has been obtained, recorded, or accessed in the same transaction or occurrence shall be punishable as a Class 6 felony. Any violation of subsection B where 50 or more persons' identifying information has been obtained, recorded, or accessed in the same transaction or occurrence shall be punishable as a Class 5 felony. Any violation resulting in the arrest and detention of the person whose identification documents or identifying information were used to avoid summons, arrest, prosecution, or to impede a criminal investigation shall be punishable as a Class 6 felony. Upon conviction, in addition to any other punishment, a person found guilty of this offense shall be ordered by the court to make restitution as the court deems appropriate to any person whose identifying information was appropriated or to the estate of such person. Such restitution may include the person's or his estate's actual expenses associated with correcting inaccuracies or errors in his credit report or other identifying information.

U.S. Federal Cybersecurity Market Forecast 2010-2015

As the Federal Information Security Management Act of 2002 enters its seventh year, it is clear that agencies and departments are not yet secure. The Government Accountability Office (GAO) continues to find security weaknesses at agencies. The President commissioned an extensive review of the plans, programs, and activities underway that address security of the government's communications and information. We forecast the deployment of a strategic framework to integrate, resource, and coordinate governments' cybersecurity efforts in the years to come, with wide participation of both government and private sectors. The following cybersecurity initiatives are being launched by the Federal Government:

- OMB Review of Agency IT security Business Cases
- Evaluation of Security Metrics
- Reviewing Current Cyber-Security Activities
- Homeland Security Presidential Directive 12 (HSPD-12)
- Securing the National Information Infrastructure
- Protecting Privacy

Market Research Media forecasts that the U.S. Federal Cybersecurity market will grow steadily – at about 6.2% CAGR over the next six years.