UNCLASSIFIED

FEDERAL UTILITY PARTNERSHIP WORKING GROUP SEMINAR

April 19-20, 2018
Nashville, TN

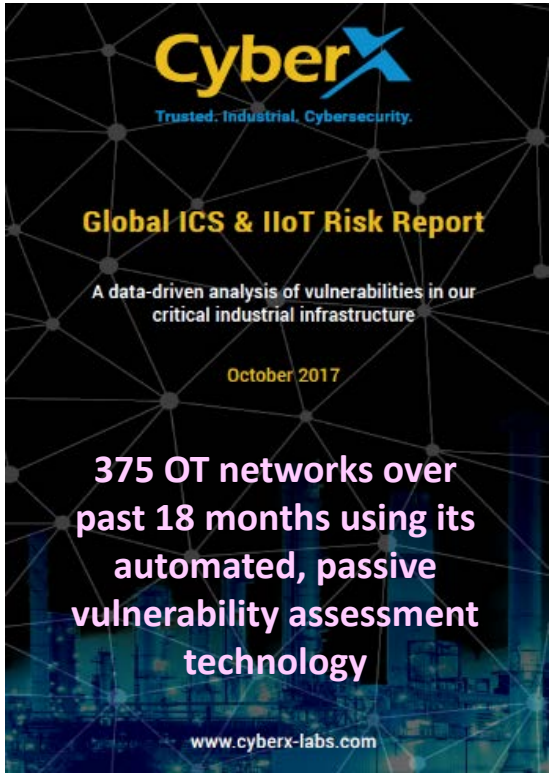
Cybersecurity – Why Bother?

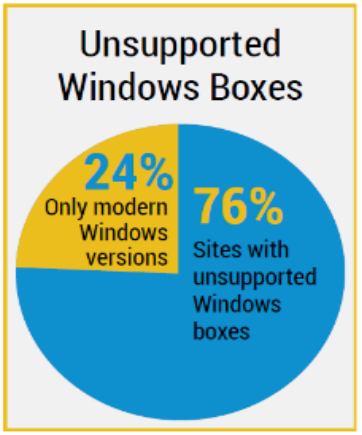
Hosted by:

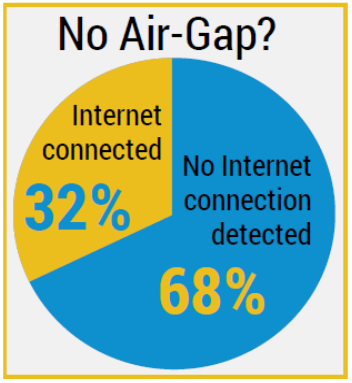
FEMP
Federal Energy Management Program

TVA

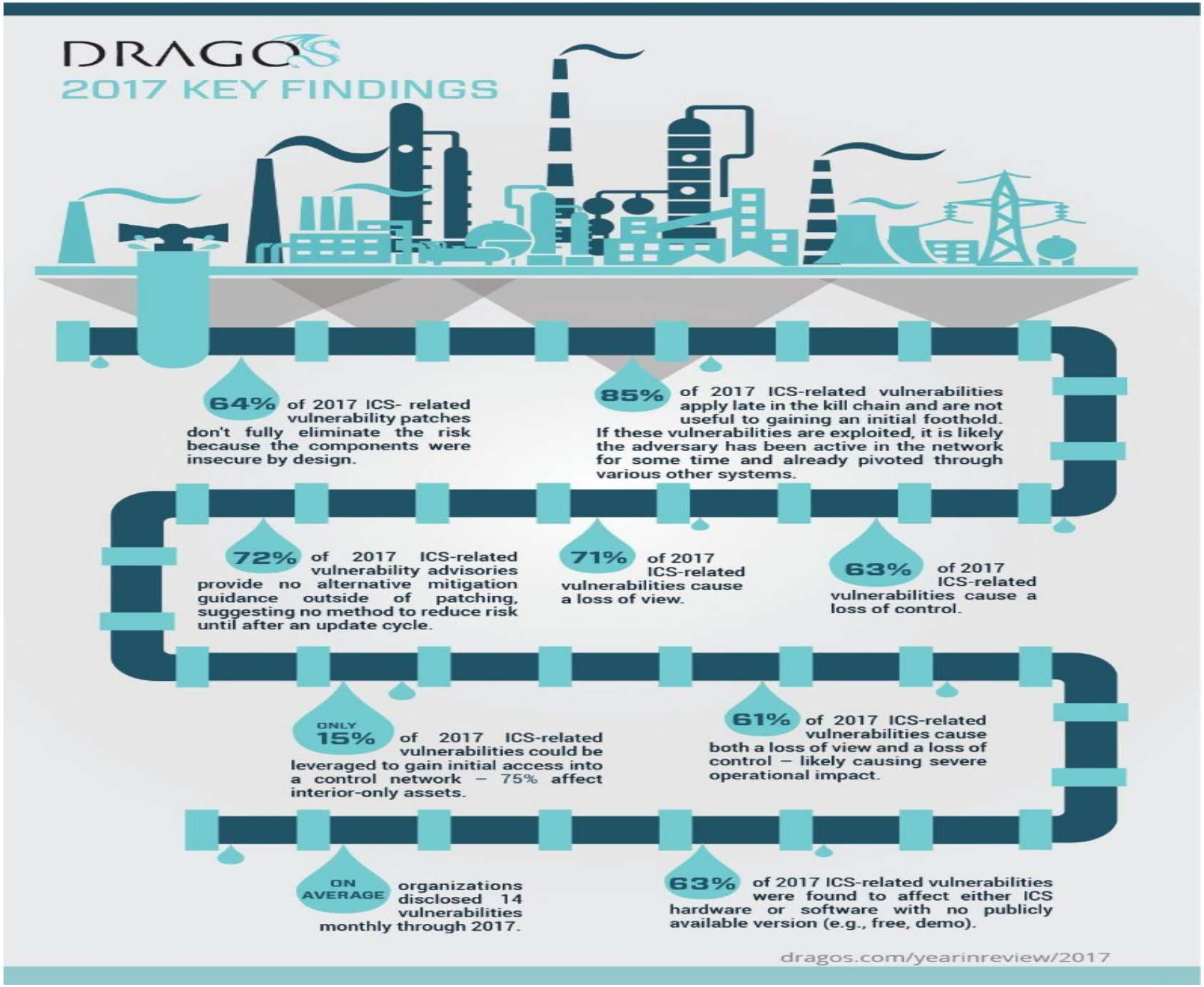
- 60% have plain-text passwords traversing their control networks
- 50% aren't running any AV protection
- Nearly 50% have at least one unknown or rogue device
- 20% have wireless access points
- 28% of all devices in each site are vulnerable
- 82% of industrial sites are running remote management protocols





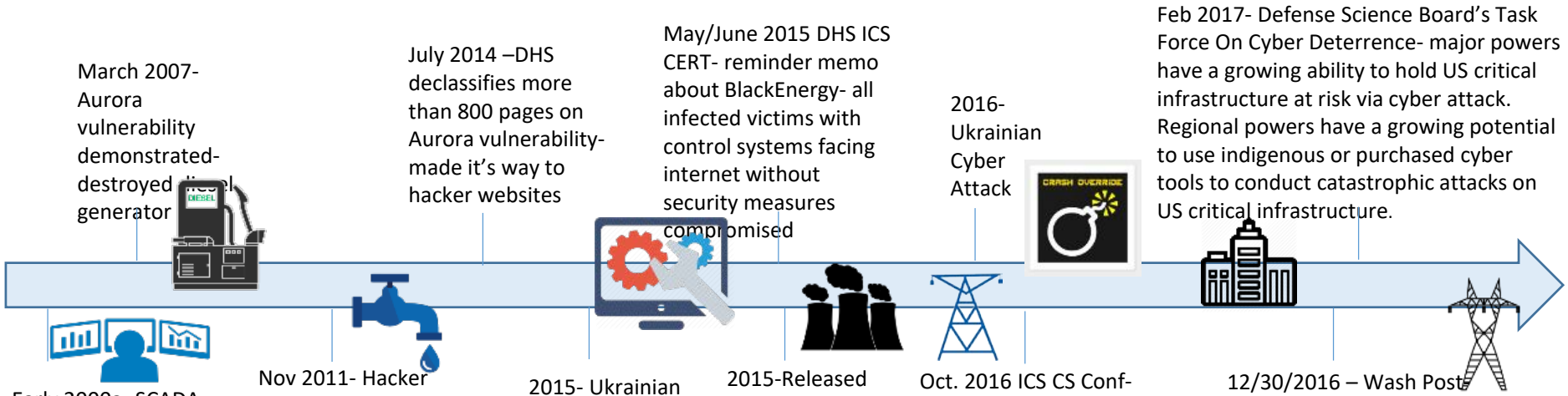


"They're testing out red lines, what they can get away with. You push and see if you're pushed back. If not, you try the next step." *Thomas Rid, Professor of War Studies at King's College London*


DRAGOS
2017 KEY FINDINGS
64% of 2017 ICS- related vulnerability patches don't fully eliminate the risk because the components were insecure by design.
85% of 2017 ICS-related vulnerabilities apply late in the kill chain and are not useful to gaining an initial foothold. If these vulnerabilities are exploited, it is likely the adversary has been active in the network for some time and already pivoted through various other systems.
72% of 2017 ICS-related vulnerability advisories provide no alternative mitigation guidance outside of patching, suggesting no method to reduce risk until after an update cycle.
71% of 2017 ICS-related vulnerabilities cause a loss of view.
63% of 2017 ICS-related vulnerabilities cause a loss of control.
ONLY 15% of 2017 ICS-related vulnerabilities could be leveraged to gain initial access into a control network – 75% affect interior-only assets.
61% of 2017 ICS-related vulnerabilities cause both a loss of view and a loss of control – likely causing severe operational impact.
ON AVERAGE organizations disclosed 14 vulnerabilities monthly through 2017.
63% of 2017 ICS-related vulnerabilities were found to affect either ICS hardware or software with no publicly available version (e.g., free, demo).
dragos.com/yearinreview/2017

The Electric Grid Continues To Be Vulnerable and Susceptible to Catastrophic Impacts

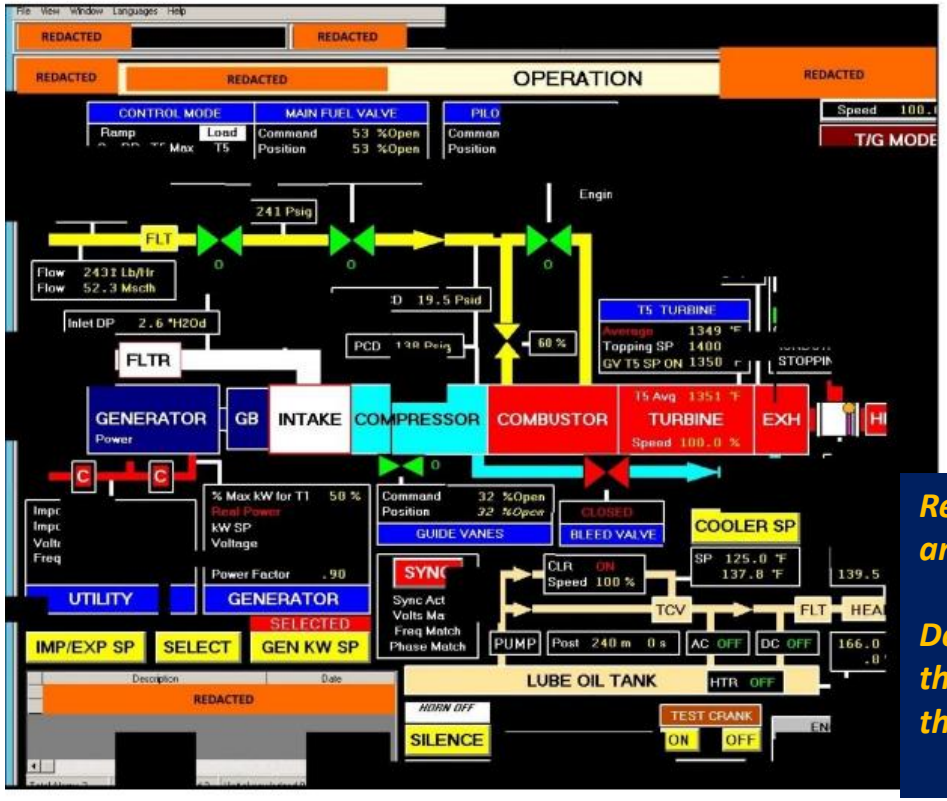
March 15, 2018, the Trump administration announced sanctions against Russian entities for a multitude of actions, including persistent attempts to break into the US electric grid.



Can Cyber Attacks Cause Outages Worth Caring About?

Russia Hacks US ICS for Critical Infrastructure

- **Russian intelligence breached computer systems for the electricity grid and conducted network reconnaissance.**
- **Targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks.**



"We now have evidence they're sitting on the machines, connected to industrial control infrastructure, that allow them to effectively turn the power off or effect sabotage," "From what we can see, they were there. They have the ability to shut the power off. All that's missing is some political motivation," -Eric Chien, security technology director at Symantec.

Recommend: Develop policies and defenses to discover, mitigate and recover from future exploits no matter the "who"

Deterrence is only possible if a potential attacker believes that they will get caught and face some kind of consequence....what's the consequence of exploiting your control system?

Utility Insight to Customer Side of Meter

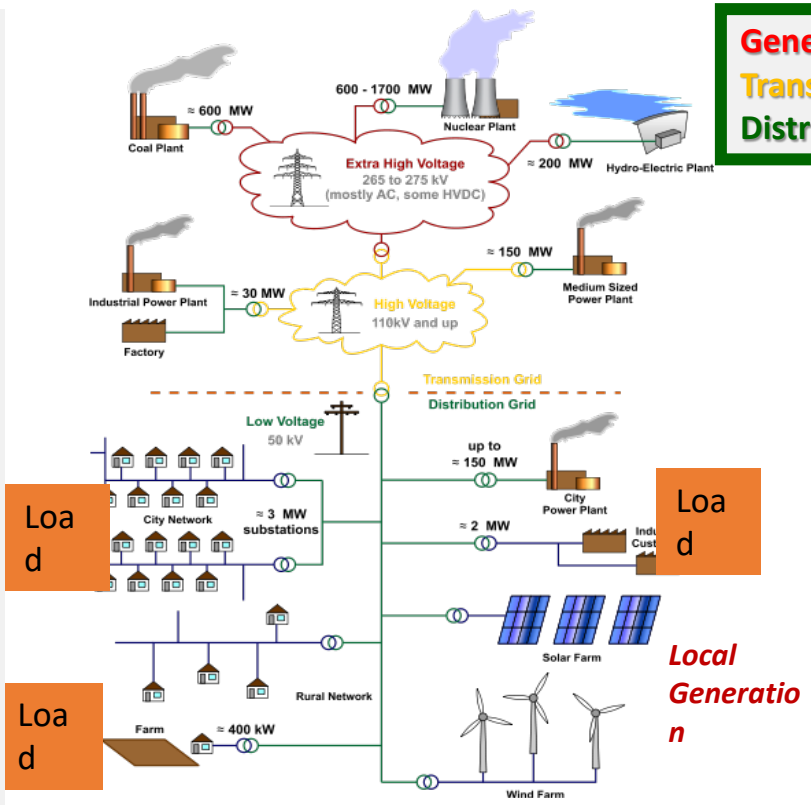
- What risks exist from IoT devices embedded in?
  - Substations
  - Customer Distributed Energy Resources (DER)
  - Internet-connected commercial and industrial devices
- Can they be hacked, infected, captured and controlled, recruited into botnets?
- Result: Launching of simultaneous demand and supply attacks and resulting in these devices being used to manipulate power flows at the edge of the grid

Possible? What / Who Should Detect, Mitigate & Recover?

Privatized Utilities Cybersecurity Proposal

"All Department energy contracts, including UP contracts, are subject to these requirements. Contractors have 60 days from date of contract award or modification to contract where the DFAR 252.204-7012 being amended to produce the following Cyber Risk Management Plan (CRMP) artifacts:

1. **System Security Plan (SSP)**
2. **Plan of Action and Milestones (POA&M)**
3. **Incident Response Plan and Procedures**
4. **Data Handling& Marking policy"**



Valuable Data Must be Protected – Use NIST SP 800.171 as Guide

NIST SP 800-171 Cyber Risk Management Plan (CRMP)

Tab 1	**Cybersecurity Requirements/Contracts**
Tab 1a	Corporate Risk Management Plan
Tab 1b	Corporate Risk Management NFPA 1600 Business Impact Analysis
Tab 1c	DoD DFARS Controlled Unclassified Information Guide 2015
Tab 1d	Client Contracts
Tab 2	**Information System Technology Policies and Procedures**
Tab 2a	Roles and Responsibilities
Tab 2b	Information Security Program Management
Tab 2c	IS Policies
Tab 2d	Acceptable Encryption
Tab 2e	Account Management
Tab 2f	Audit Policy
Tab 2g	Awareness and Training
Tab 2h	Configuration Management
Tab 2i	Email Policy
Tab 2j	Information Sensitivity
Tab 2k	Password Construction

Tab 2m	Penetration Testing
Tab 2n	Remote Access
Tab 2o	Software Installation
Tab 2p	Vulnerability Management
Tab 2q	Wireless Communication
Tab 2r	Wireless Communication Standard
Tab 2s	Workstation Security
Tab 3	**Corporate Cybersecurity Plans and Procedures**
Tab 3a	Corporate System Security Plan (SSP)
Tab 3b	Corporate Plan Of Action and Milestones (POAM)
Tab 3c	Corporate Information Systems Contingency Plan / CONOPS (ISCP)
Tab 3d	Corporate Event/Incident Communication Plan (EICP)
Tab 3e	Corporate Event/Incident Response Plan (EIRP)
Tab 3f	Corporate Security Audit Plan (SAP) Procedures
Tab 3g	Corporate Security Monthly Audit Report (SMAR) Procedures
Tab 3h	DBINet DFARS Incident Response Form
Tab 3i	US-CERT Incident Response Form
Tab 3k	CJCSM 6510.01B - Cyber Incident Handling Program 2012 Incident Response Form

NERC Proposed Reliability Standards for Supply Chain Security (Sept' 17)

Measures designed to:

- **Reduce likelihood that vendor patch updates could be exploited;**
- **Address remote access threats, such as stolen credentials or threat that a compromised vendor could traverse over an unmonitored connection into a Bulk Electric System ("BES");**
- **Address risk that unsecure equipment could be inadvertently installed;**
- **Address risk that responsible entities could make risky contracts and purchases that fail to meet minimum security criteria; and**
- **Address risk that vendors might not have adequate notification processes or response mechanisms in place.**

Require Responsible Entities to Manage their Supply Chain Cyber Risks & Develop Risk Management & Response Plans to Address any Breakdown in Procurement, Installation or Transfers Between Vendors

Cybersecurity for Energy Delivery Systems (CEDS) Partnerships

Asset Owners/Operators

- Ameren
- Arkansas Electric Cooperatives Corporation
- Avista
- Burbank Water and Power
- BPA
- CenterPoint Energy
- Chevron
- ComEd
- Dominion
- Duke Energy
- Electric Reliability Council of Texas
- Entergy
- FirstEnergy
- FP&L
- HECO
- Idaho Falls Power
- Inland Empire
- Omaha Public Power District
- Orange & Rockland Utility
- Pacific Gas & Electric
- PacifiCorp
- Peak RC
- PJM Interconnection
- Rochester Public Utilities
- Sacramento Municipal Utilities District
- Electric
- Sempra
- Snohomish PUD
- Southern Company
- Southern California Edison
- TVA
- Virgin Islands Water and Power Authority
- WAPA
- Westar Energy
- WGES

Solution Providers

- ABB
- Alstom Grid
- Applied Communication Services
- Applied Control Solutions
- Cigital, Inc.
- Critical Intelligence
- Cybati
- Eaton
- Enernex
- EPRI
- San Diego Gas and Electric
- Foxguard Solutions
- GE
- Grid Protection Alliance
- Grimm
- Honeywell
- ID Quantique
- Intel
- NexDefense
- OPAL-RT
- Open Information Security Foundation
- OSIsoft
- Parsons
- Power Standards Laboratory
- Qubitekk
- RTDS Technologies Inc.
- Schneider Electric
- SEL
- Siemens
- Telvent
- Tenable Network Security
- Utility Advisors
- Utility Integration Solutions
- UTRC
- Veracity
- ViaSat

Academia

- Arizona State University
- Carnegie Mellon University
- Dartmouth College
- Florida International University
- Georgia Institute of Technology
- Illinois Institute of Technology
- Iowa State University
- Lehigh University
- Massachusetts Institute of Technology
- Oregon State University
- Rutgers University
- Tennessee State University
- Texas A&M EES
- University of Arkansas
- University of Arkansas-Little Rock
- University of Buffalo - SUNY
- University of Illinois
- UC Davis
- UC Berkeley
- University of Houston
- University of Tennessee-Knoxville
- University of Texas at Austin
- Washington State

National Labs

- Argonne National Laboratory
- Brookhaven National Laboratory
- Idaho National Laboratory
- Lawrence Berkeley National Laboratory
- Lawrence Livermore National Laboratory
- Los Alamos National Laboratory
- National Renewable Energy Laboratory
- Oak Ridge National Laboratory
- Pacific Northwest National Laboratory
- Sandia National Laboratories

Other

- Energy Sector Control Systems Working Group
- International Society of Automation
- NESCOR
- NRECA
- Open Information Security Foundation

Example Outcomes for Tomorrow's Resilient Energy Delivery Systems

U.S. DEPARTMENT OF ENERGY | Office of Electricity Delivery & Energy Reliability

EXAMPLE OUTCOMES

Tools and technologies to anticipate future grid scenarios, design in cybersecurity, and enable power systems to automatically recognize and reject a cyber attack:

- → Architectures that secure the cyber interaction of grid-edge devices and data streams in the cloud
- → Resilient building energy management systems that can switch to a more secure platform during a potential cyber incident
- → A cyber-physical control and protection architecture for multi-microgrid systems that enable stable grid performance during a cyber attack using electrical islands
- → Resilient operational networking technology that automates cyber incident responses

Build strategic core capabilities at 10 National Laboratories and build multi-university collaborations dedicated to advancing Energy Delivery Systems cybersecurity

EXAMPLE OUTCOMES

Tools and technologies to *prevent* cyber attacks:

- → Quantum key distribution to securely exchange data using cryptographic keys while detecting attempted eavesdropping
- → Algorithms that continuously and autonomously assess and reduce the cyber attack surface

Tools and technologies to *detect* cyber attacks:

- → Rapid anomaly identification that may indicate a compromise in utility control communications
- → Tools to detect spoofing or compromise of the precise GPS time signals used for synchrophasor data

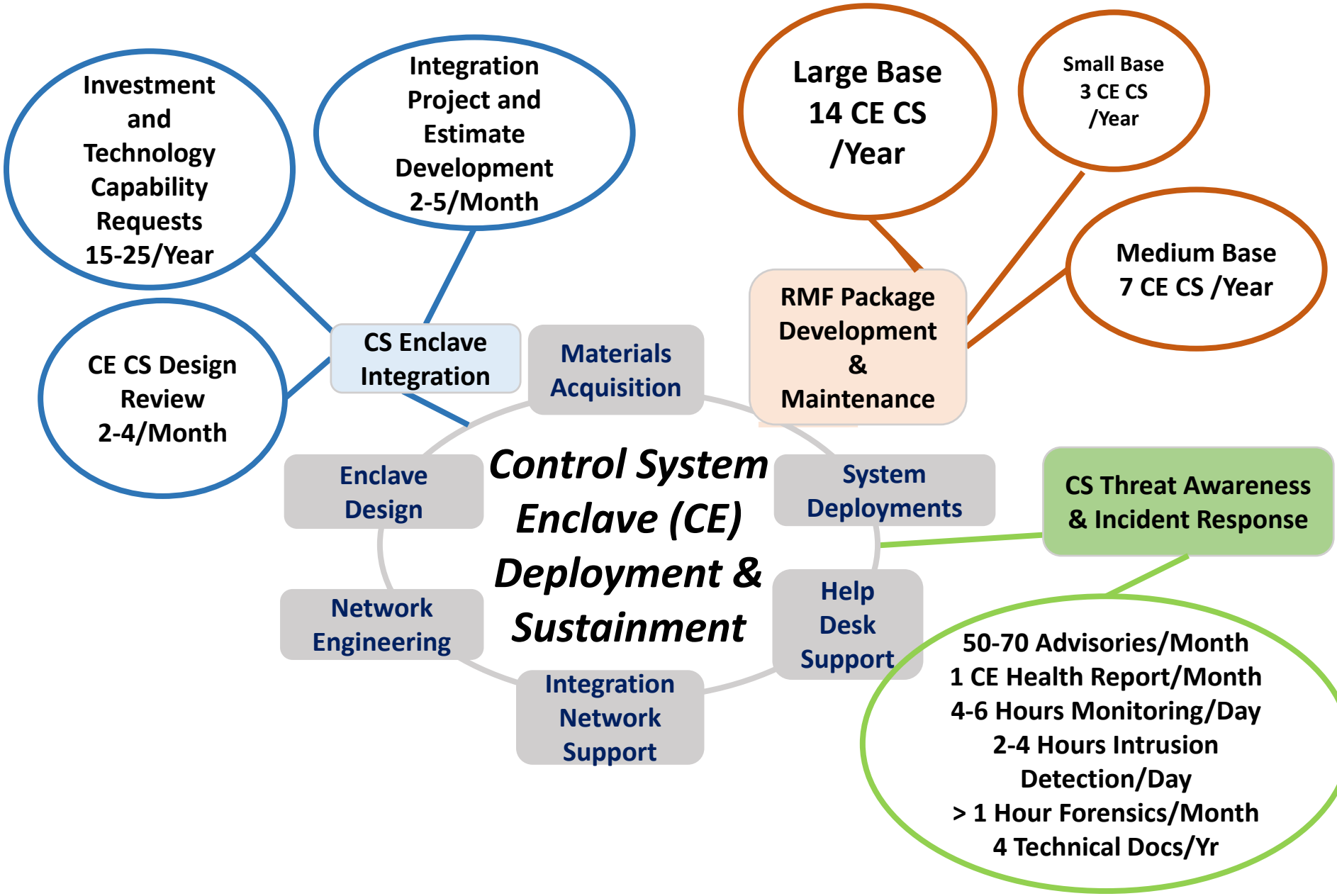
Tools and technologies to *mitigate* cyber attacks:

- → Ability for high-voltage DC systems to detect when commands could destabilize the grid and reject the command or take a different action
- → Network risk assessment model to classify attacks based on impact potential and **assess network's resilience to zero-day attacks**

UT-04	Control Systems (CS)	Identify control systems for all utilities, processes, and machinery. Ensure control systems have adequate physical and cybersecurity protection. (See Cybersecurity Operations Benchmarks and ensure CYBEROPS benchmarks are applies to identified control systems.)	DoDI 8510.01 DoDI 8500.01 DoDI 8530.01 UFC 4-010-06 NIST 800-30 NIST 800-37 NIST 800-82 NIST 800-53
UT-05	Supporting Infrastructure Dependencies	Identify dependencies on and support provided to other supporting foundational infrastructure networks (SFINs) out to at least one node away from the installation perimeter, including electricity, bulk fuel storage, natural gas, road, rail, air, and water transportation, communications, potable water, heating, ventilation, and air conditioning, chemicals, and munitions. Include material and service contracted support.	DoDI 3020.45 DoDD 3020.26 DoDI 4170.11 DoDI 6055.16

CYBEROPS-10	Platform IT - Control Systems (PIT-CS)	PIT-CS, Facility-Related Control Systems (FRCS), and Operational Technology (OT) supporting the critical assets have appropriate procedural, security, technical, and administrative measures for the criticality and sensitivity level of the systems. (All Cybersecurity benchmarks maybe utilized to assess control systems as a network. Coordinate with Supporting Infrastructure benchmarks for operation of systems).	CJCSI 6510.01F DoDI 8500.01 DoDI 8510.01 NIST SP 800-82

AFCEC Cybersecurity RFP Scope



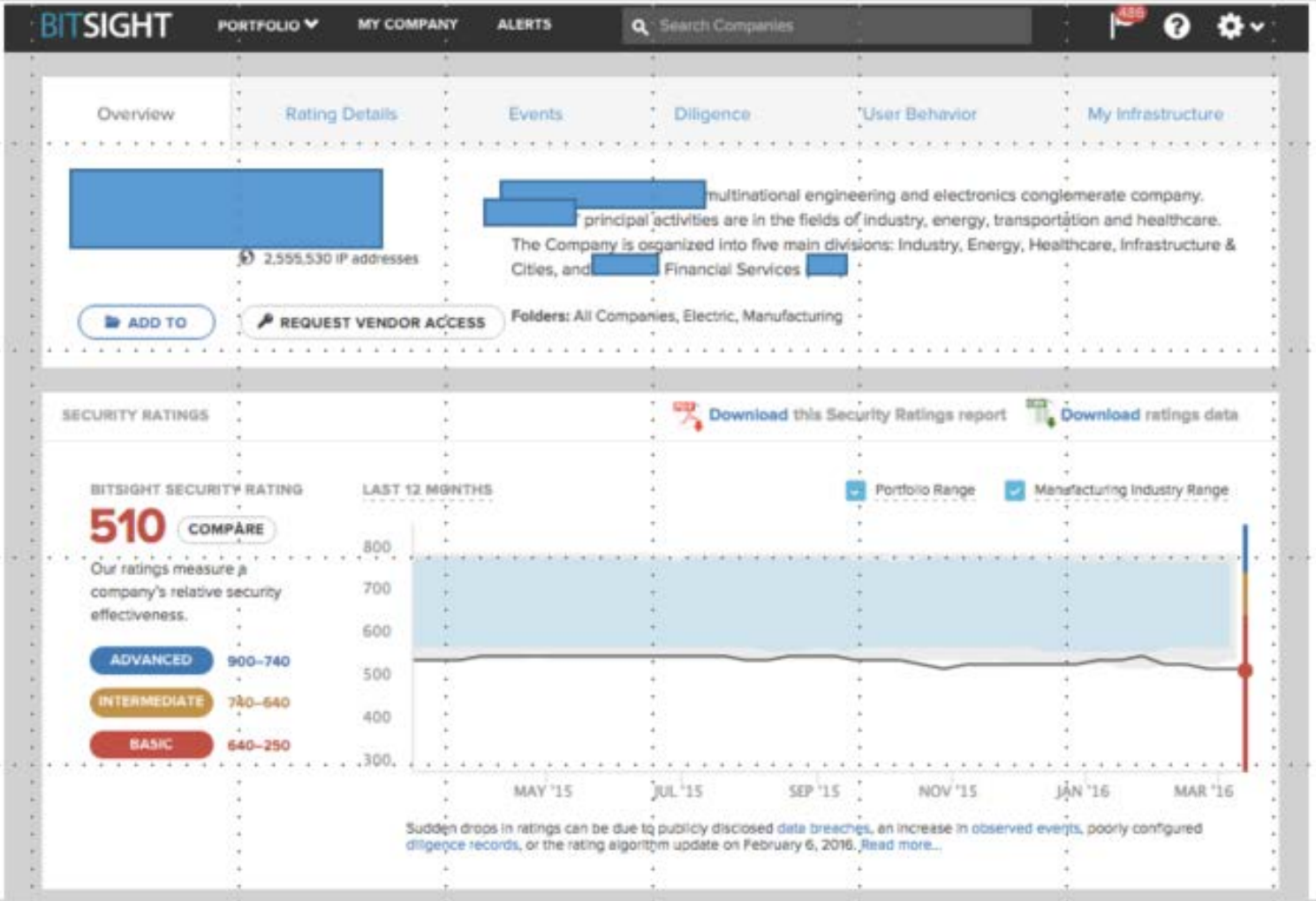
What's Your Cyber 'Risk' or 'Trust' Score?

- Bitsight — bitsighttech.com
- Risk Recon — riskrecon.com
- Security Scorecard — securityscorecard.com
- Upguard — upguard.com

- **Use public information & network signatures for FICO score-like rating approximating relative risk**
- **Enables intelligence for evaluation of critical suppliers, vendors, and others in the industry**
- **Augments Business Intelligence Unit and Security Operations Center; ques alerts to potential cyber or physical threats to our supply chains and internal infrastructure**
- **Each vendor's approach & scores roughly similar**
- **Need to verify accuracy – may detect one or more notables that were not really present in the enterprise under evaluation (e.g. a sub-domain or IP address not really associated with the target)**
- **<u>Benefit / Objectives</u>: Credibility approaching supplier/partner with security issue; avoid false positives & decrease time to investigate and mitigate**

Which $ Decisions Be Based on Cyber Performance?

BitSight Rating Interface



BITSIGHT

Detailed Event and Configuration Information on 3rd Parties

EVENTS

Botnet Infections	F
Spam Propagation	B
Malware Servers	A
Unsolicited Communication	B
Potentially Exploited	C

DILIGENCE

SPF Domains	C
DKIM Records	F
TLS/SSL Certificates	C
TLS/SSL Configurations	B
Open Ports	C
DNSSEC Records beta	C
Application Security beta	C

USER BEHAVIOR

File Sharing	D

OTHER

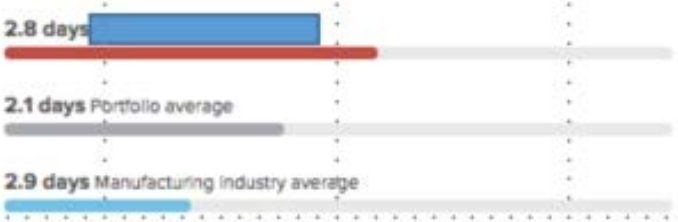
Data Breaches	A

EVENTS

Events are observed incidents of compromise on a company's network. These include risk vectors such as botnet infections and malware servers. Industry averages are calculated from similarly sized companies.

THIS WEEK	PAST YEAR	AVERAGE EVENT DURATION
10	1,416	2.8 days

3.4% faster to resolve events than the Manufacturing industry average.



File Sharing category distribution

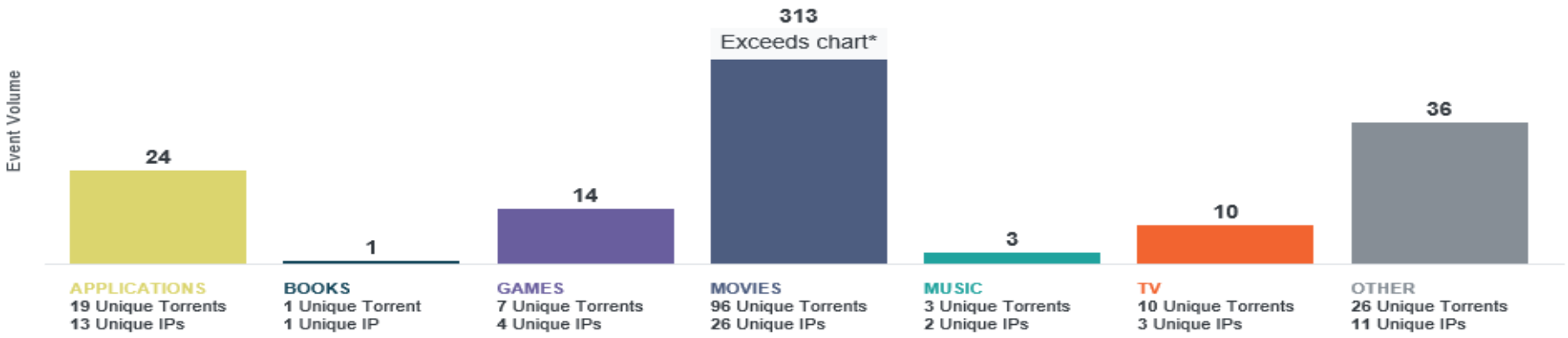
File Sharing events indicate the number of times in the past 60 days that file sharing activity occurred, sorted by torrent category. Each event represents one IP address sharing one torrent per day.

F
Grade

in the bottom 10% of all companies

File Sharing – 401 events over the past 60 days
40 unique IPs observed

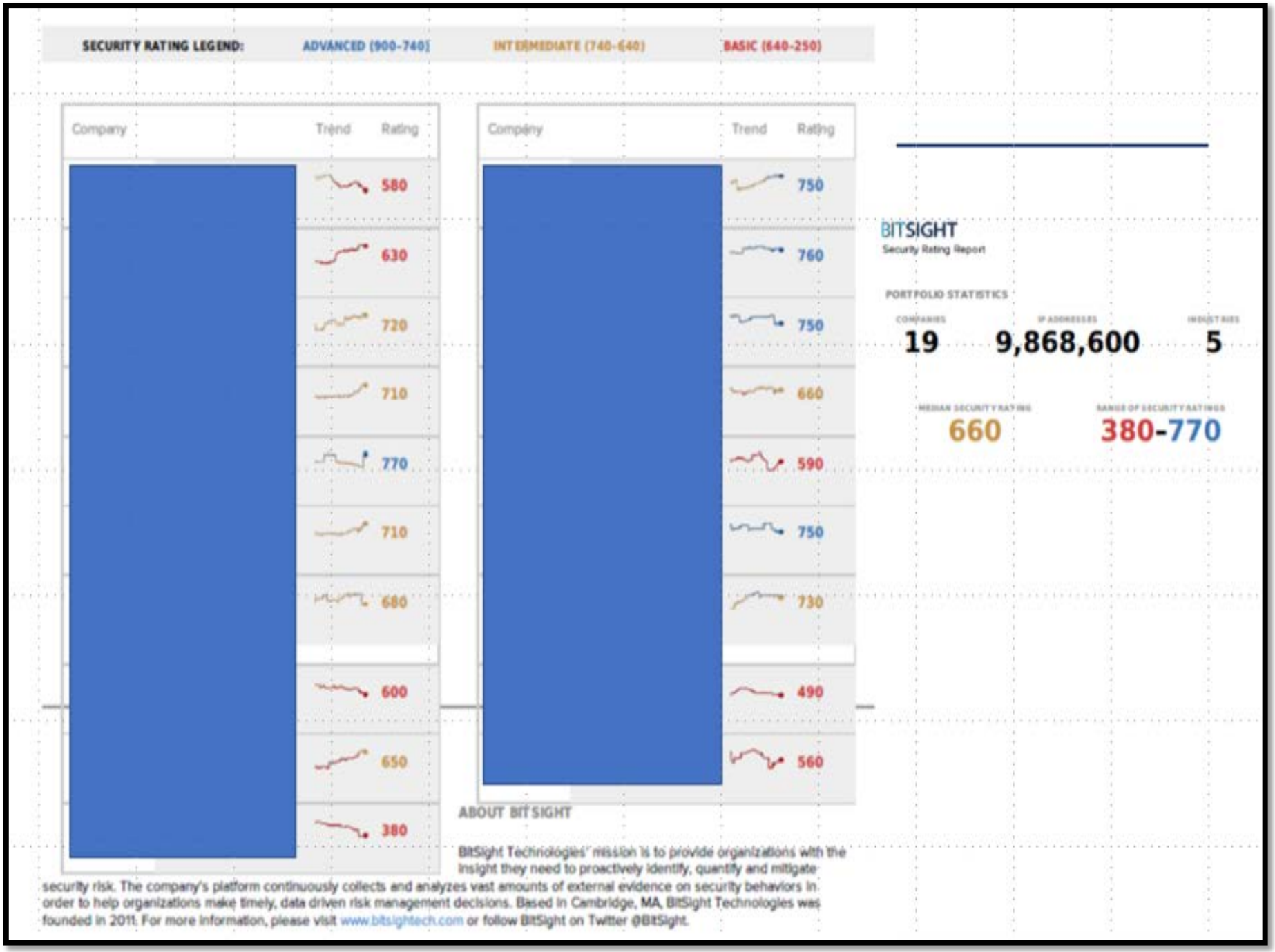
*Data which exceeds the chart is on a scale too large to display accurately with other categories in the space provided and has been shortened to fit.



Search | From MM-DD-YYYY | to MM-DD-YYYY | Filter Results: All Categories | Only Impacts Grade

Filter By Tags

File Sharing Category	Start	End	Impacts Grade	Days	Whitelisted
Applications	03-29-2018	03-29-2018		1	No
Music	03-28-2018	03-28-2018		1	No
Movies	03-27-2018	03-27-2018		1	No


SECURITY RATING LEGEND:
ADVANCED (900-740)
INTERMEDIATE (740-640)
BASIC (640-250)
Company
Trend
Rating
580
630
720
710
770
710
680
600
650
380
Company
Trend
Rating
750
760
750
660
590
750
730
490
560
BITSIGHT
Security Rating Report
PORTFOLIO STATISTICS
COMPANIES
19
IP ADDRESSES
9,868,600
INDUSTRIES
5
MEDIAN SECURITY RATING
660
RANGE OF SECURITY RATINGS
380-770
ABOUT BITSIGHT
BitSight Technologies' mission is to provide organizations with the insight they need to proactively identify, quantify and mitigate security risk. The company's platform continuously collects and analyzes vast amounts of external evidence on security behaviors in order to help organizations make timely, data driven risk management decisions. Based in Cambridge, MA, BitSight Technologies was founded in 2011. For more information, please visit www.bitsightech.com or follow BitSight on Twitter @BitSight.

Discussion

FEMP Federal Energy Management Program

TVA