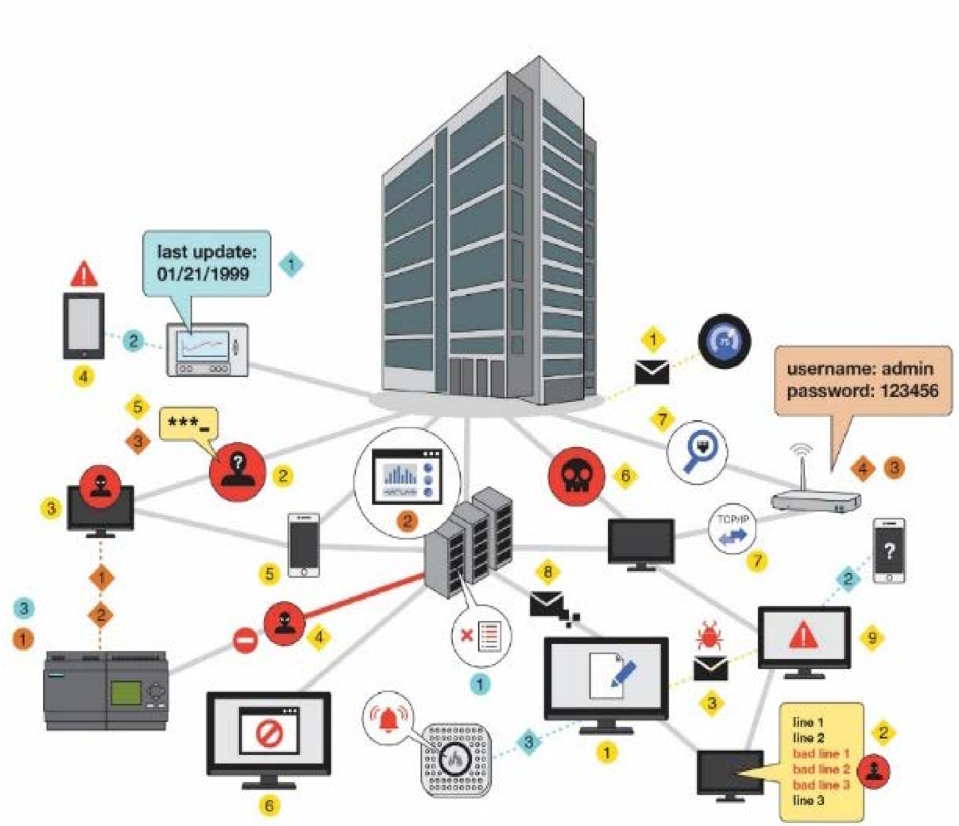
Buildings Cybersecurity Opportunities, Challenges and Solutions



MICHAEL MYLREA

Manager, Cybersecurity & Energy Technology

Pacific Northwest National Lab

November 2, 2016

Acknowledgements

Many Thanks to:

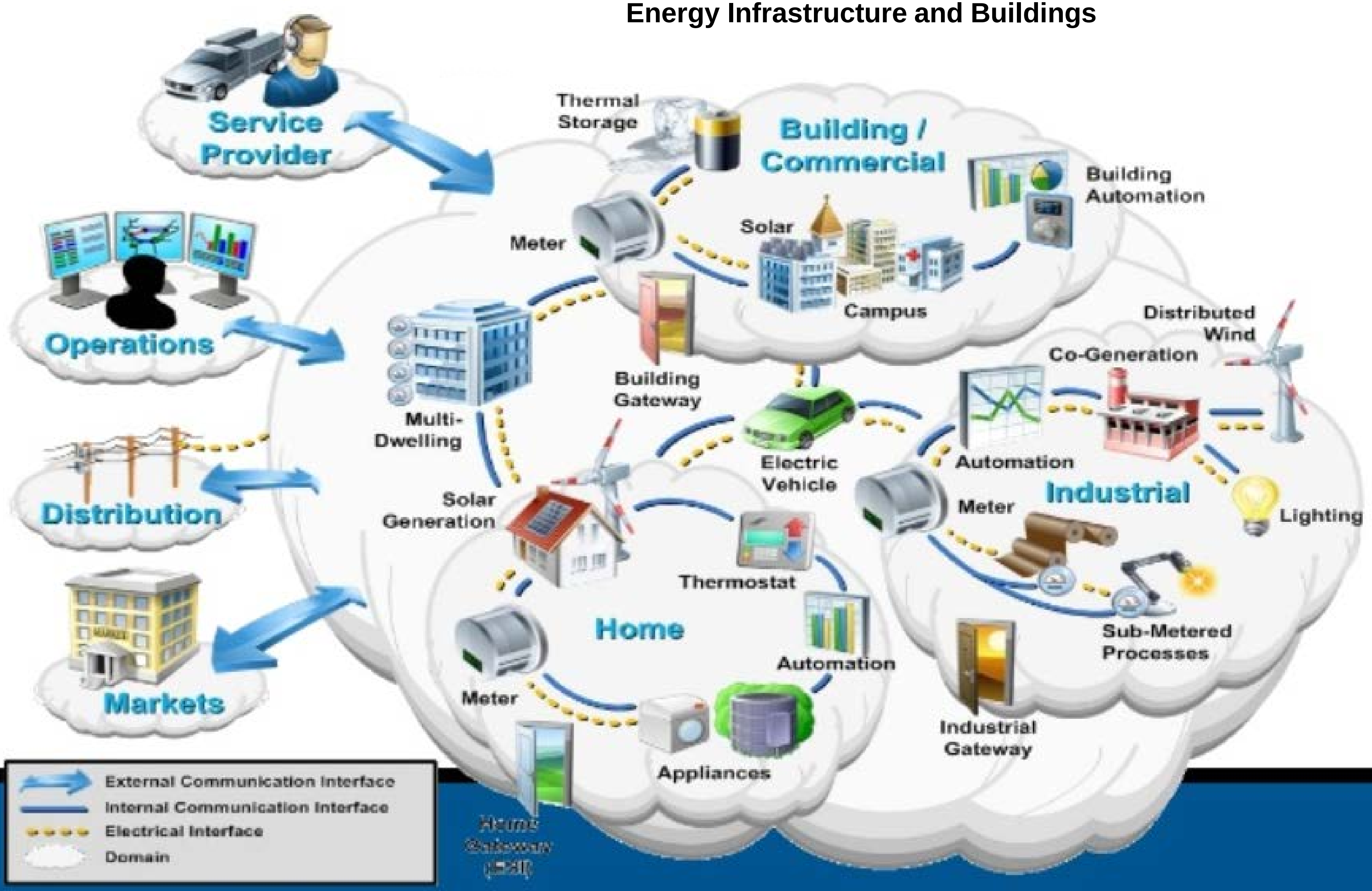
- The U.S. Department of Energy’s Federal Energy Management Program (**Dr. Tim Unruh**); Building Technologies Office (**Joe Hagerman**) and Energy’s Office of Electricity and Energy Reliability (**Dr. Carol Hawk**) for supporting PNNL Buildings and Energy Technology Cybersecurity efforts

- Federal Utility Partnership Working Group (FUPWG) Participants and Sponsors

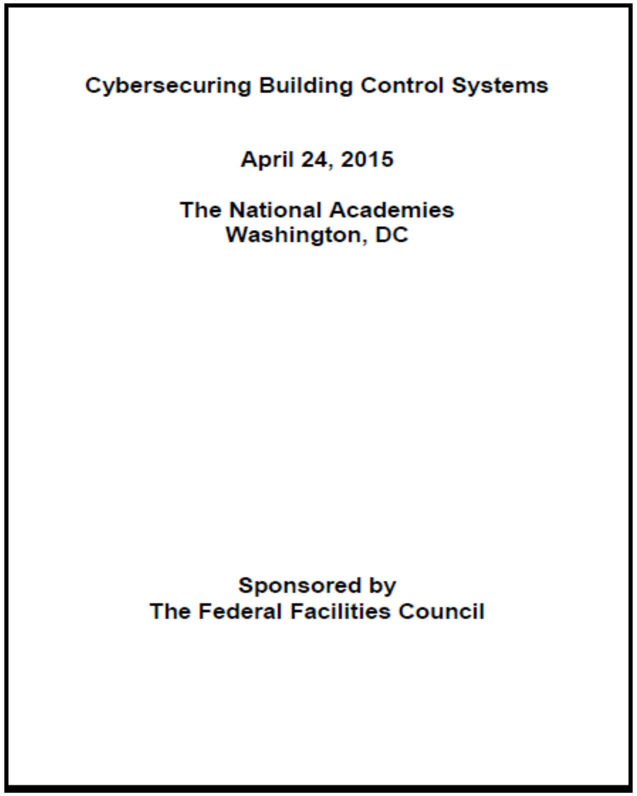
Buildings Cybersecurity Opportunities & Challenges

All Modern Organizations Are Cyber & Energy Organizations

Cyber And Physical Systems, IT and OT, are Converging In Energy Infrastructure and Buildings



National Academies Identifies "Connected Buildings = Vulnerable"



Cybersecuring Building Control Systems

April 24, 2015

The National Academies
Washington, DC

Sponsored by
The Federal Facilities Council

"**The nation's buildings are increasingly relying on building control systems with embedded communications technology and many enabled via the Internet**. These systems provide critical services that allow a building to meet the functional and operational needs of building occupants, but they can also be easy targets for hackers and people with malicious intent. These facilities contain building and access control systems such as heating, ventilation, and air conditioning; electronic card readers…that are increasingly being automated and connected to other information systems or networks and the Internet. **As these systems are becoming more connected, so is their vulnerability to potential cyber-attacks."**

DOE EERE Approach: Secure + Connected = Economic, Energy, Environment Opportunity

1. Engage industry and Federal agencies to define the problem and better understand the gaps in a very complex space of connected devices and buildings

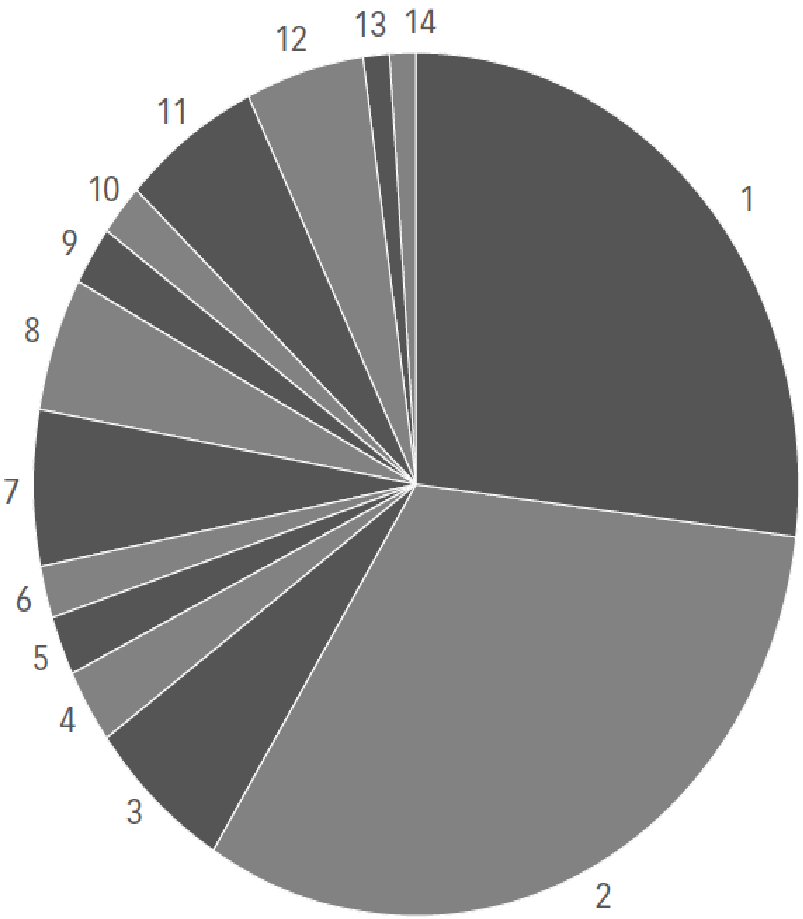
2. Develop easy to use framework to help buildings stakeholders establish cybersecurity policies, procedures and cybersecurity controls (Building Cybersecurity Framework)

3. Develop tool to measure and improve existing policies, cybersecurity awareness, readiness and risk management (B-C2M2)

Buildings Include Several Critical Infrastructures Experiencing Increased Cyber Attacks, according DHS

Figure 8: ICS cyber incidents reported to ICS-CERT, 2014

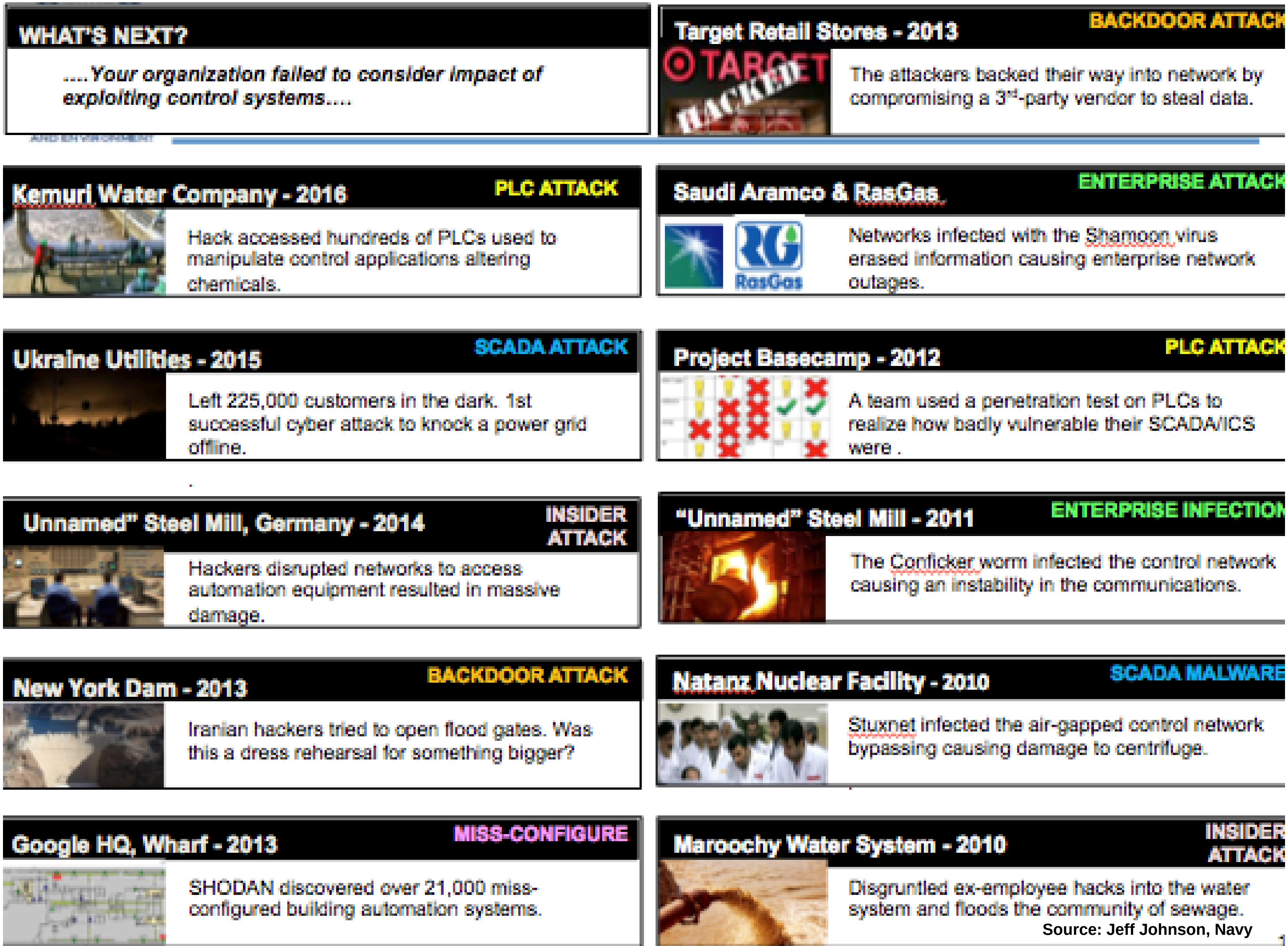
Source: US Department of Homeland Security, 'ICS-CERT Year in Review'



Buildings include several of the sixteen critical infrastructures designated by EO 13636, including commercial facilities, financial services, government facilities, healthcare and public health and information technology.

	Sector	%
1	Critical manufacturing	27
2	Energy	32
3	Communications	6
4	Commercial facilities	3
5	Chemical	2
6	Unknown	2
7	Water	6
8	Transportation	5
9	Nuclear	2
10	Information technology	2
11	Healthcare	6
12	Government facilities	5
13	Finance	1
14	Agriculture	1

Operational Technology Cyber Incidents – What’s Next?



WHAT'S NEXT?

....Your organization failed to consider impact of exploiting control systems....

Target Retail Stores - 2013 — BACKDOOR ATTACK

The attackers backed their way into network by compromising a 3rd-party vendor to steal data.

Kemuri Water Company - 2016 — PLC ATTACK

Hack accessed hundreds of PLCs used to manipulate control applications altering chemicals.

Saudi Aramco & RasGas — ENTERPRISE ATTACK

Networks infected with the Shamoon virus erased information causing enterprise network outages.

Ukraine Utilities - 2015 — SCADA ATTACK

Left 225,000 customers in the dark. 1st successful cyber attack to knock a power grid offline.

Project Basecamp - 2012 — PLC ATTACK

A team used a penetration test on PLCs to realize how badly vulnerable their SCADA/ICS were .

Unnamed" Steel Mill, Germany - 2014 — INSIDER ATTACK

Hackers disrupted networks to access automation equipment resulted in massive damage.

"Unnamed" Steel Mill - 2011 — ENTERPRISE INFECTION

The Conficker worm infected the control network causing an instability in the communications.

New York Dam - 2013 — BACKDOOR ATTACK

Iranian hackers tried to open flood gates. Was this a dress rehearsal for something bigger?

Natanz Nuclear Facility - 2010 — SCADA MALWARE

Stuxnet infected the air-gapped control network bypassing causing damage to centrifuge.

Google HQ, Wharf - 2013 — MISS-CONFIGURE

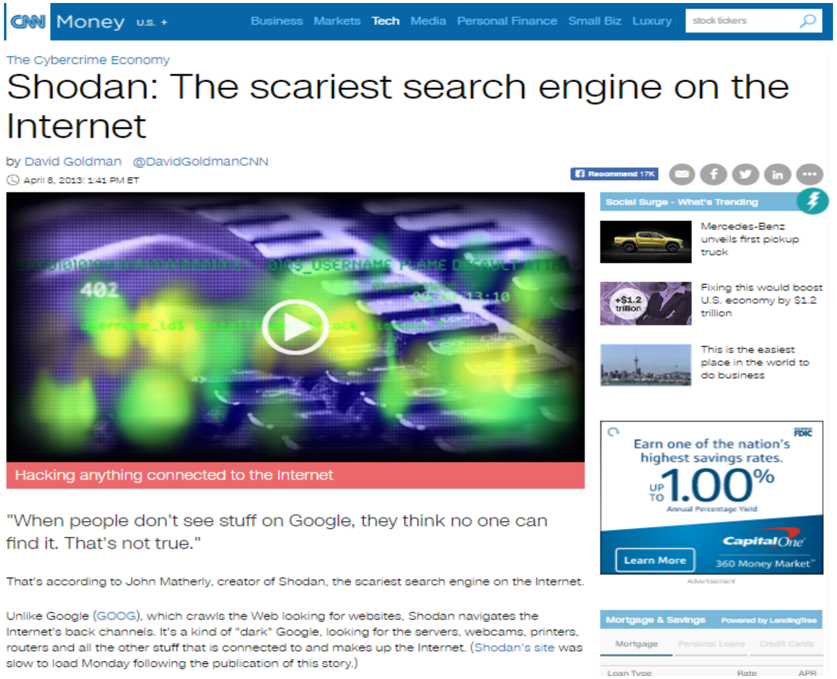
SHODAN discovered over 21,000 miss-configured building automation systems.

Maroochy Water System - 2010 — INSIDER ATTACK

Disgruntled ex-employee hacks into the water system and floods the community of sewage.

Source: Jeff Johnson, Navy

Shodan: Search Engine to Hack or Secure Vulnerable Buildings Technology?



The Cybercrime Economy

Shodan: The scariest search engine on the Internet

by David Goldman @DavidGoldmanCNN

April 8, 2013: 1:41 PM ET

Hacking anything connected to the Internet

"When people don't see stuff on Google, they think no one can find it. That's not true."

That's according to John Matherly, creator of Shodan, the scariest search engine on the Internet.

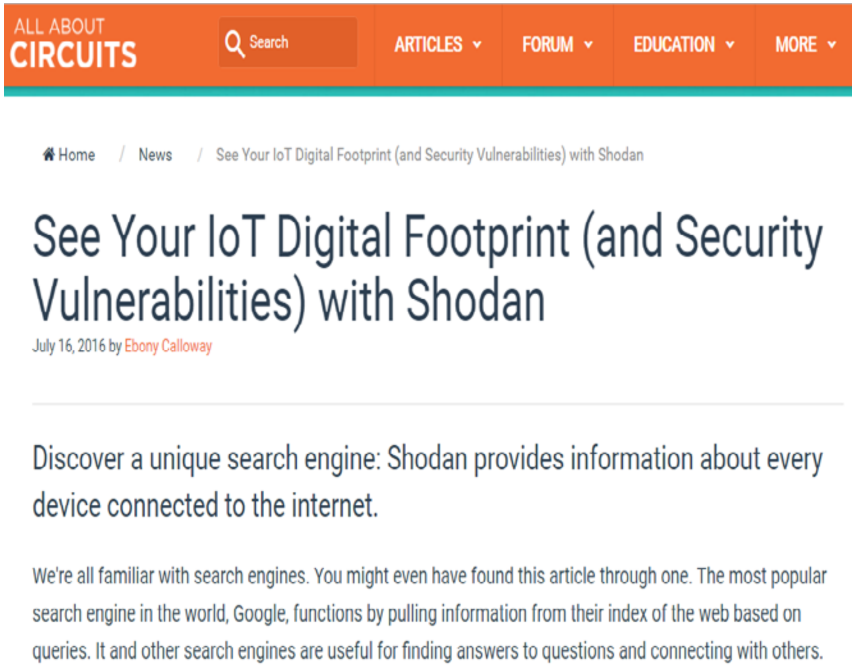
Unlike Google (GOOG), which crawls the Web looking for websites, Shodan navigates the Internet's back channels. It's a kind of "dark" Google, looking for the servers, webcams, printers, routers and all the other stuff that is connected to and makes up the Internet. (Shodan's site was slow to load Monday following the publication of this story.)

Social Surge - What's Trending

Mercedes-Benz unveils first pickup truck

Fixing this would boost U.S. economy by $1.2 trillion

This is the easiest place in the world to do business


ALL ABOUT CIRCUITS
Search
ARTICLES
FORUM
EDUCATION
MORE
Home / News / See Your IoT Digital Footprint (and Security Vulnerabilities) with Shodan

See Your IoT Digital Footprint (and Security Vulnerabilities) with Shodan

July 16, 2016 by Ebony Calloway

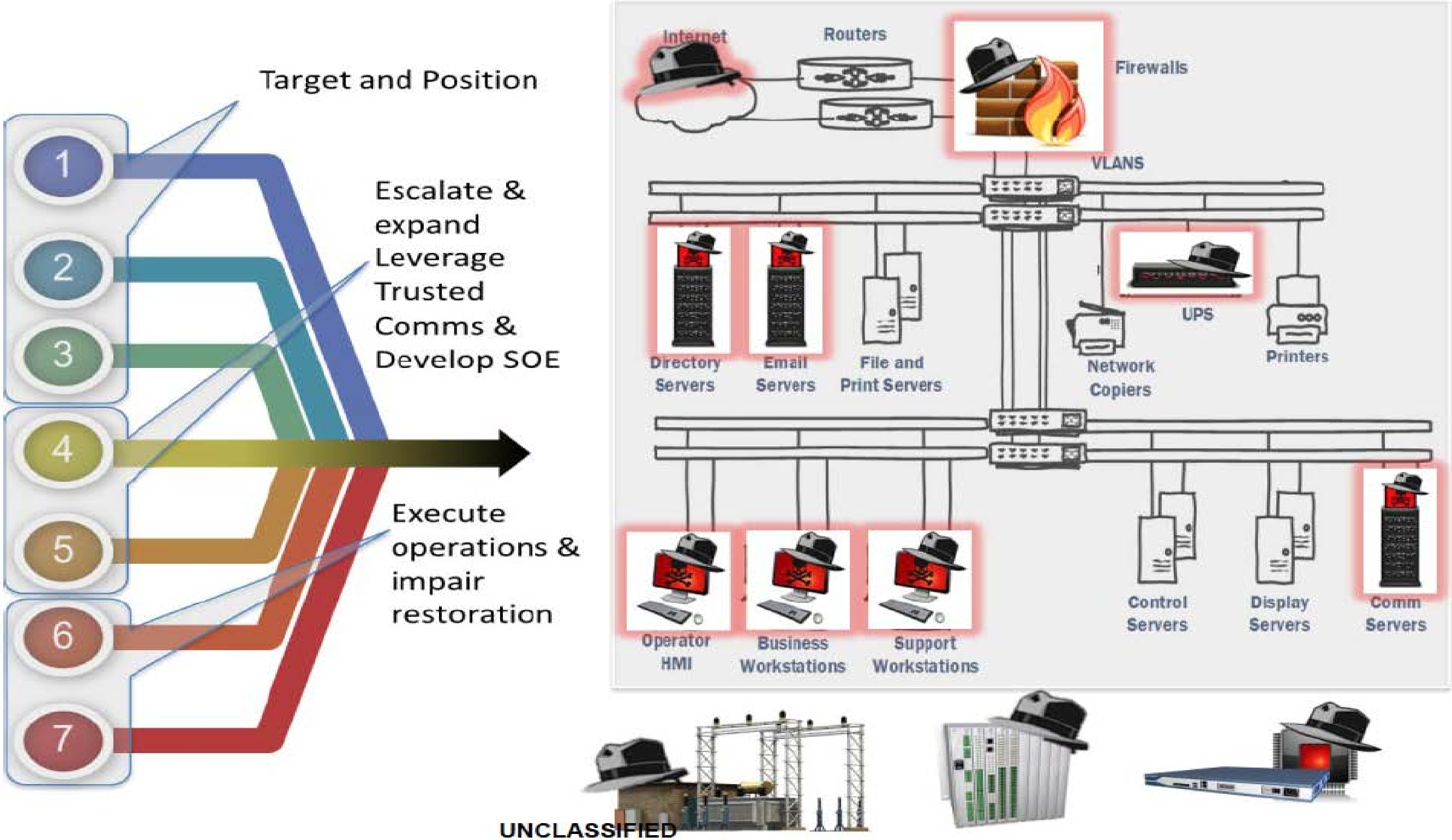
Discover a unique search engine: Shodan provides information about every device connected to the internet.

We're all familiar with search engines. You might even have found this article through one. The most popular search engine in the world, Google, functions by pulling information from their index of the web based on queries. It and other search engines are useful for finding answers to questions and connecting with others.

Shodan search engine quickly finds thousands of vulnerable building automation systems

Ukraine Cyber Attack – Included a Building Cyber Events

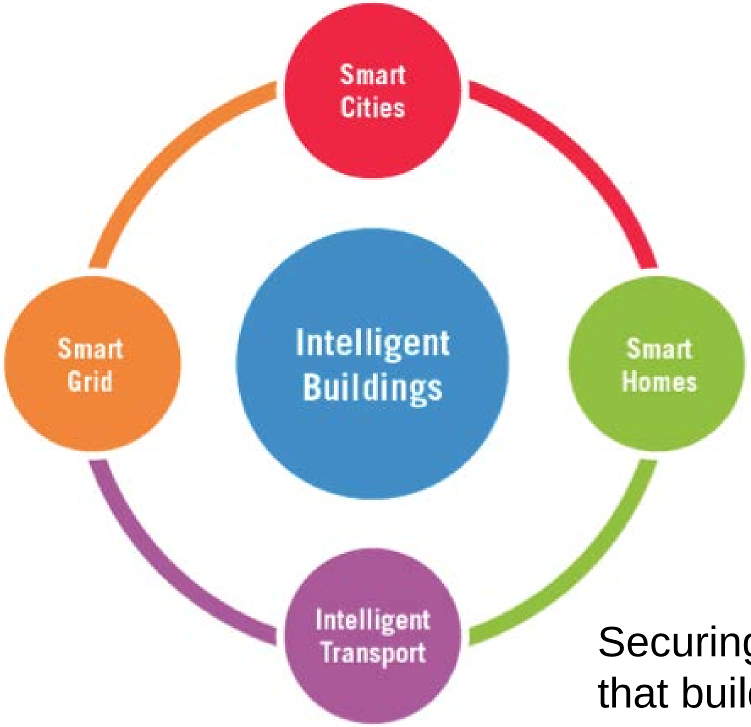
Attackers discovered a network connected to a UPS and reconfigured it so that when the attacker caused a power outage, it was followed by an event that would also **impact the power in the energy company's building data centers**

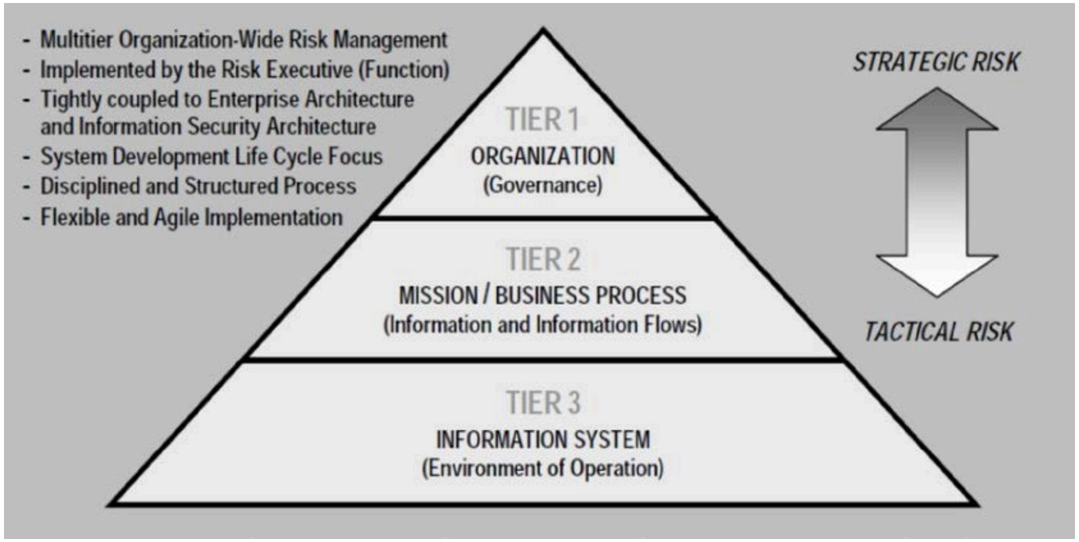


UNCLASSIFIED

Tim Conway, DOE OE

Traditional Cyber Security Paradigms Are Not Adequate To Secure Modern Buildings





- Multitier Organization-Wide Risk Management
- Implemented by the Risk Executive (Function)
- Tightly coupled to Enterprise Architecture and Information Security Architecture
- System Development Life Cycle Focus
- Disciplined and Structured Process
- Flexible and Agile Implementation

TIER 1
ORGANIZATION
(Governance)

TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)

TIER 3
INFORMATION SYSTEM
(Environment of Operation)

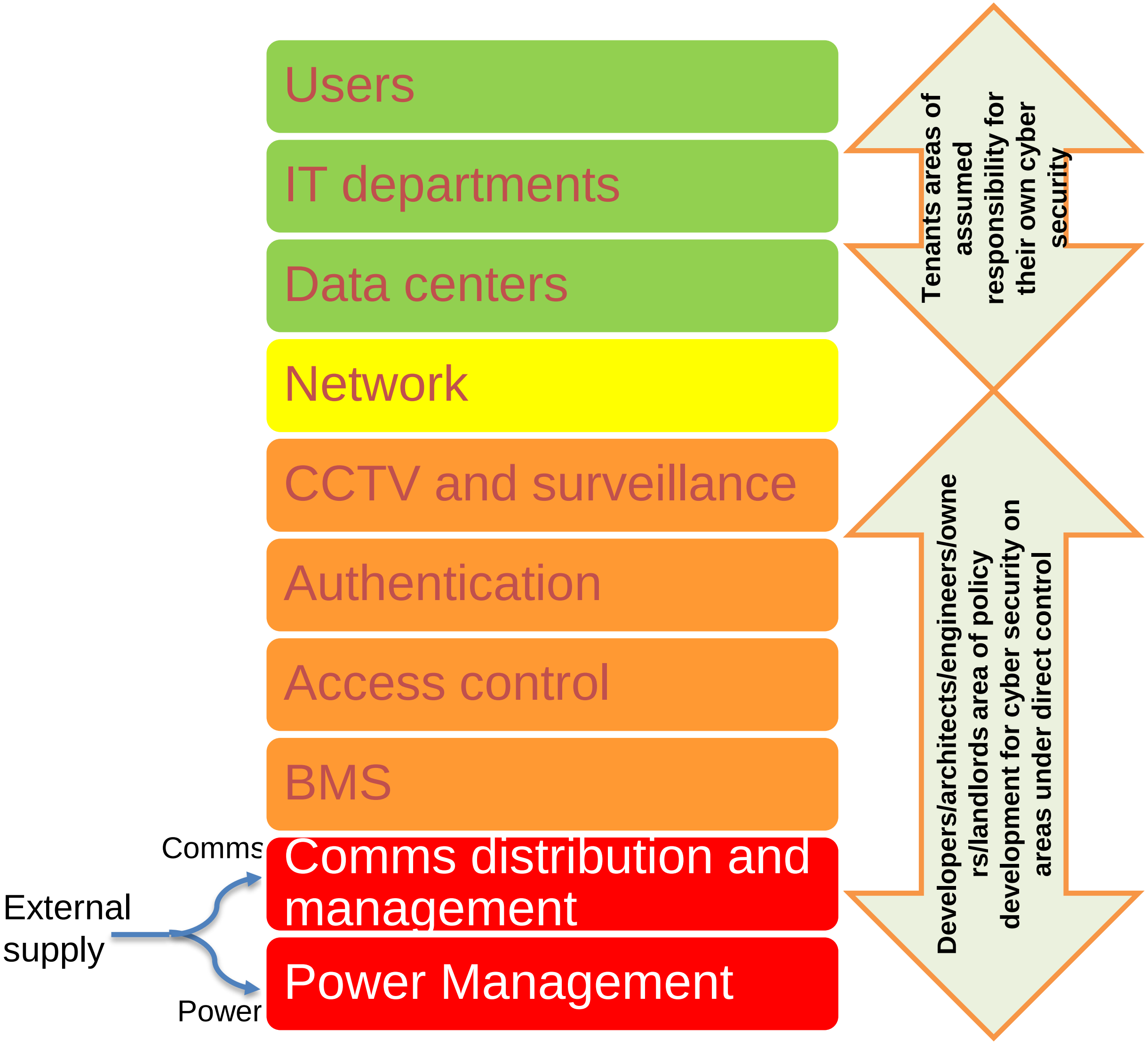
Securing smart buildings requires new security paradigms that build on and adapt existing solutions, standards and technology to better manage risk of increasingly converged OT and IT systems.

Supply Chain Challenges - Need Cyber Smart Procurement Guidelines for Buildings

- **Buildings technology continues to evolve:**
  - New cybersecurity threats and vulnerabilities
  - Changes in security practices and requirements
  - Advancing technologies
  - Expanding global supply chain
- Vendors, asset owners, operators are experiencing increased pressure for meeting stringent regulatory requirements
- Procurement can help manage risks resulting from extended and geographically dispersed **supply chains**
  - Need to build cybersecurity into solutions from the beginning
- Acquirers, integrators, and suppliers need to communicate expectations and requirements in a clear and repeatable manner

Buildings cybersecurity procurement guidelines to facilitate adoption, secure and sustainable deployment of smart buildings technology

Who Is Responsible For Securing Buildings IT and OT From Cyber Threats?



Users

IT departments

Data centers

Network

CCTV and surveillance

Authentication

Access control

BMS

Comms distribution and management

Power Management

External supply

Comms

Power

Tenants areas of assumed responsibility for their own cyber security

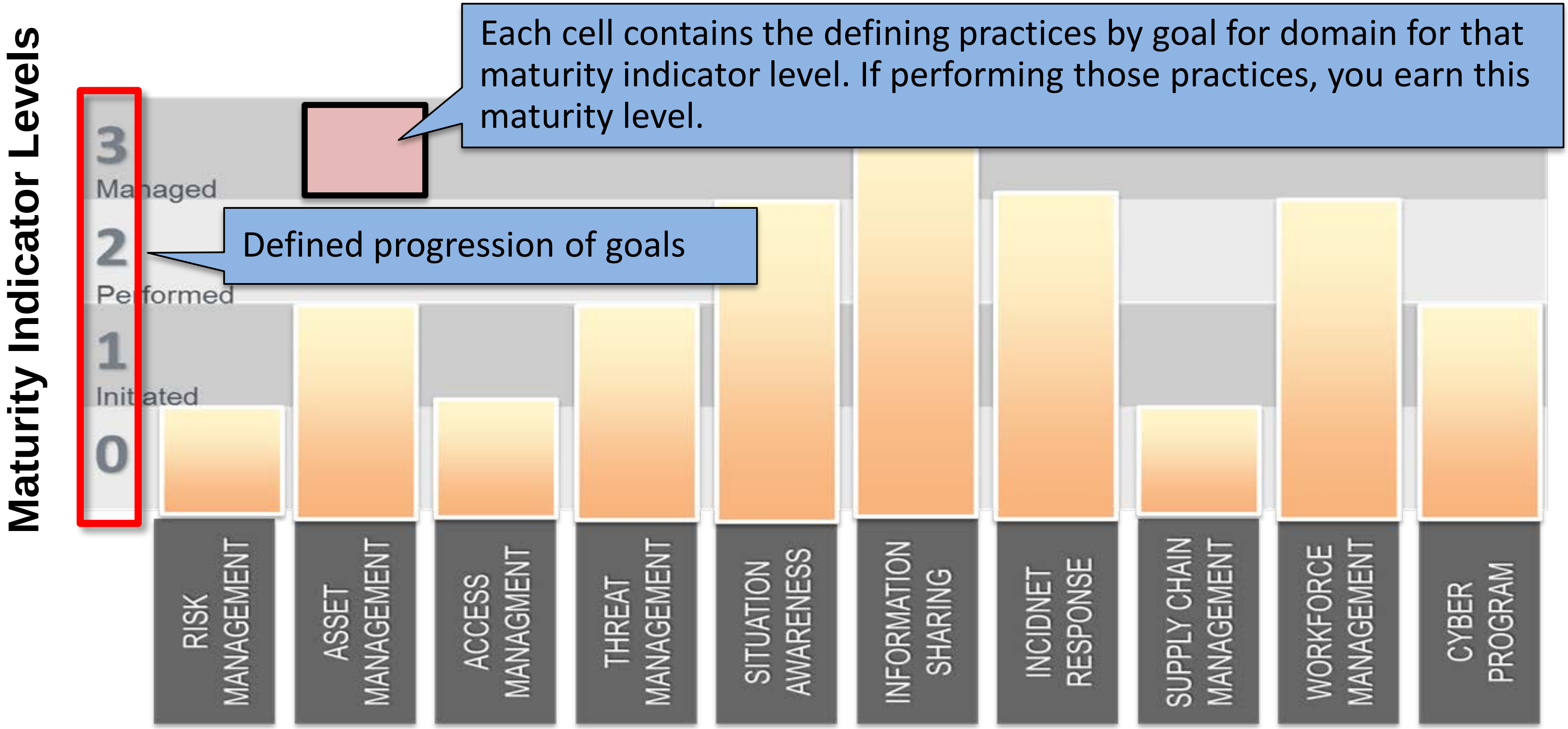
Developers/architects/engineers/owners/landlords area of policy development for cyber security on areas under direct control

Challenges in terms of organizational roles and responsibilities, introducing new operational complexity and risk into buildings that owners and operators are often not prepared to deal with.

DOE & PNNL Power Grid and Buildings Cybersecurity Efforts

Buildings Cybersecurity Maturity Model (B-C2M2)

WWW.BC2M2.PNNL.GOV



Each cell contains the defining practices by goal for domain for that maturity indicator level. If performing those practices, you earn this maturity level.

Defined progression of goals

- DOE and PNNL developed a tool and visualization platform to measure cybersecurity maturity for energy utilities. This tool has been adapted to buildings
- B-C2M2 provides a high level view of cybersecurity situational awareness and risk focusing on ten critical cyber domains
- A tool and data set for measuring and comparing nation’s buildings cybersecurity maturity does not exist

Buildings Cybersecurity Maturity Model (B-C2M2) – Includes 10 Critical Cyber Domains

RM	Risk Management
ACM	Asset, Change, and Configuration Management
IAM	Identity and Access Management
TVM	Threat and Vulnerability Management
SA	Situational Awareness
ISC	Information Sharing and Communications
IR	Event and Incident Response, Continuity of Operations
EDM	Supply Chain and External Dependencies Management
WM	Workforce Management
CPM	Cybersecurity Program Management

- Domains are logical groupings of cybersecurity practices
- Each domain has an acronym that cross references with the evaluation toolkit

Critical Cyber Domain Example 1- Supply Chain & External Dependencies Management

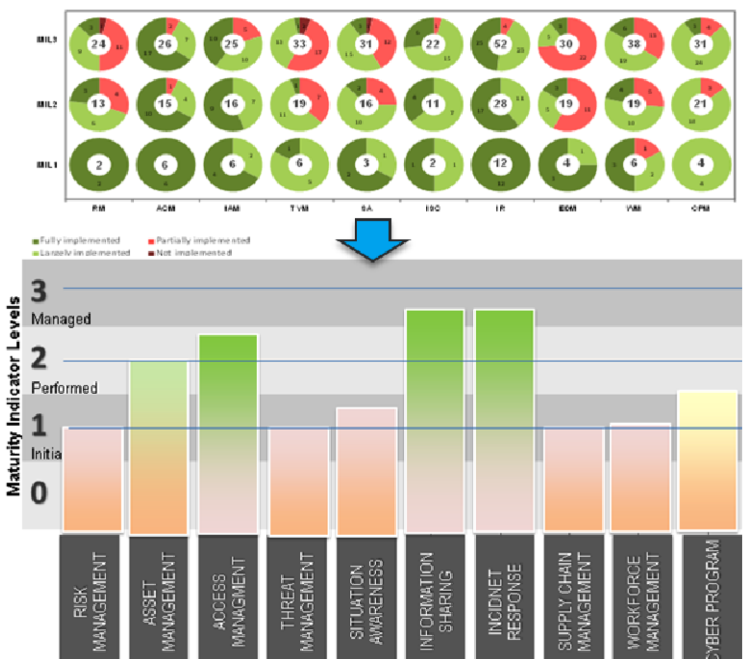
Objectives:

- Identify dependencies
- Manage dependency risk
- Management activities

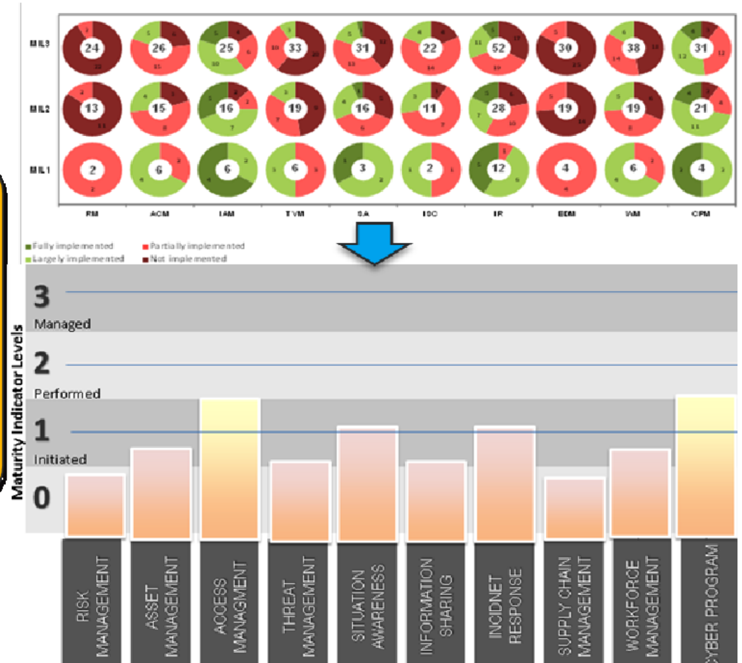
Related Questions

- Significant cybersecurity risks due to suppliers and other dependencies are identified and addressed?
- Cybersecurity requirements are considered, at when establishing relationships with suppliers and other third parties?

Highest/Lowest Maturity in Pilot Studies



No Facility-level Identifiable Information (FII) is provided or retained by DOE.



Critical Cyber Domain Example #2 - Workforce Management

Objectives:

- Assign cybersecurity responsibilities
- Control the workforce life cycle
- Develop cybersecurity workforce
- Increase cybersecurity awareness
- Management activities

Appropriate training, testing, redundancy and evaluations of performance required

Personnel vetting, assigning risk designations to positions with access to assets and employing measures to prevent wrongdoing

Training & recruiting for overcoming skill gaps

Workforce training & recruiting for overcoming skill gaps; periodic security awareness training

What is the B-C2M2?

B-C2M2…

- ✓ Is completely voluntary
- ✓ Measures the maturity of an organization’s cybersecurity capabilities
- ✓ Focuses on the programmatic structure
- ✓ Provides descriptive and flexible guidance
- ✓ Publicly available

B-C2M2 <u>IS NOT</u>…

- ✗ Required or mandated
- ✗ Guidance for implementing specific security controls
- ✗ Penetration test.
- ✗ Intended to replace other cybersecurity-related activities, programs, processes, or approaches.

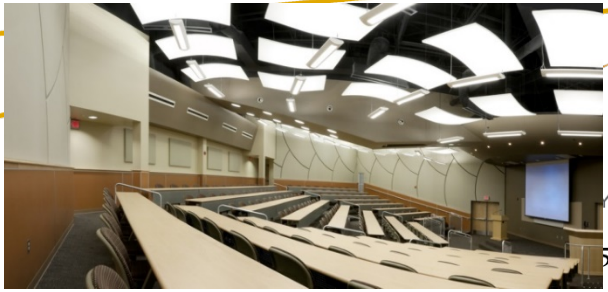
B-C2M2 Piloted in Five buildings

From Oct 2015 – April 2016 PNNL conducted pilot assessments at:

1. A **large laboratory facility** w/ many automated building control systems.

2. A **municipal building**, completed in 2011, with state-of-the-art energy and automated BCS.
3. A **university campus** with a mix of buildings (1970's - 2015) construction, many with automated BCS.

4. A **community college campus** with a mix of buildings from late 1950's – 2010's.
5. A **Federal Agency campus**



Each assessment took about 2 hours and involved interviews with senior building control system engineers, IT person, and sometimes facility manager.

Additional Lessons Learned from B-C2M2 Pilot Assessments

- **Considerable range in maturity of cybersecurity programs.**
  - **General lack of documented cybersecurity policies and procedures** for building control system security.
  - **Few resources and limited time allocated** to address cybersecurity.

- **Lack of any formal risk assessment and management program** for building control systems.
  - **Much being done right, though in ad-hoc manner**. Without continuity planning, personnel changes can drop a cybersecurity program back to square one.

- **Mature IT cyber program helps**, but does **not address all risks**.
  - **Security monitoring too limited**. Often relies on vendor software triggering of an alarm that shows an out-of-bounds condition.

- **B-C2M2 questions raised awareness**. Often heard "*I hadn't thought of that – I think I should start paying more attention to…*"

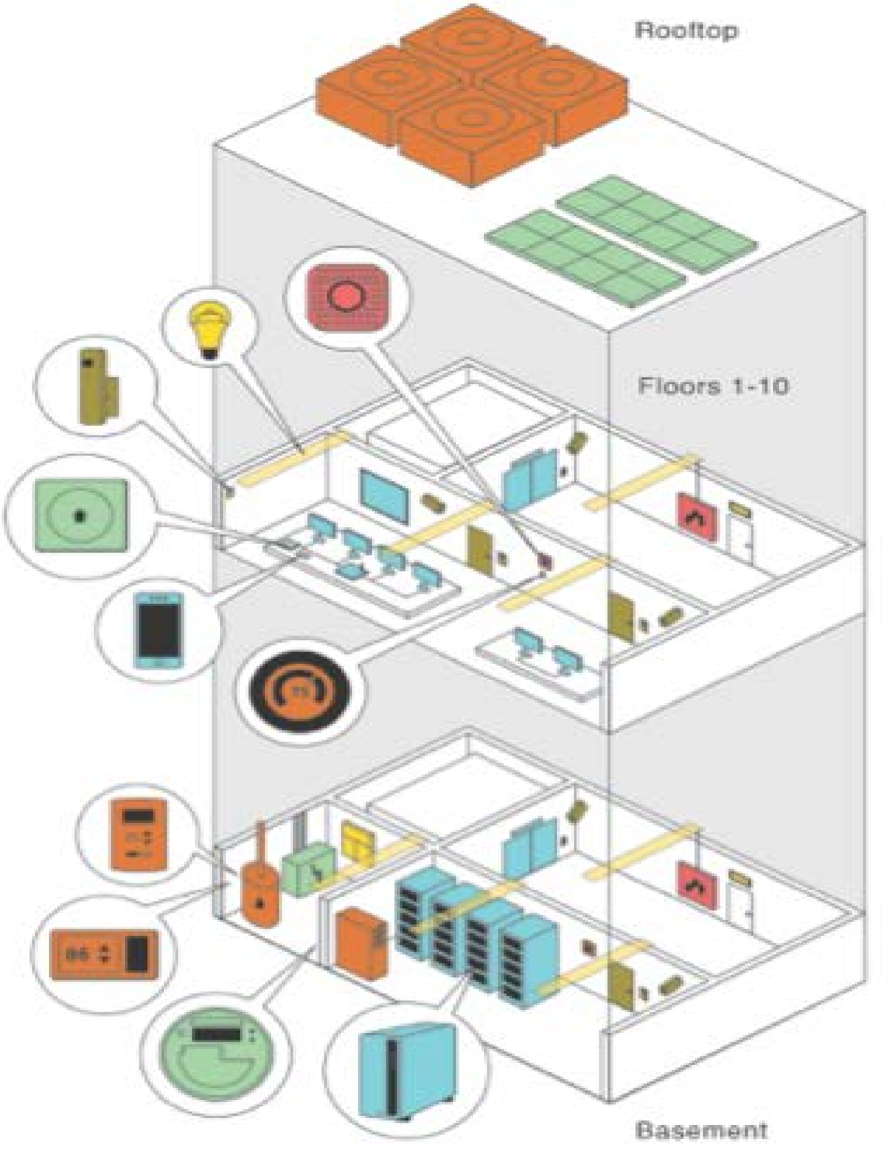
Illustrative B- C2M2 Building Cybersecurity Vulnerability Findings

Critical Asset Clusters

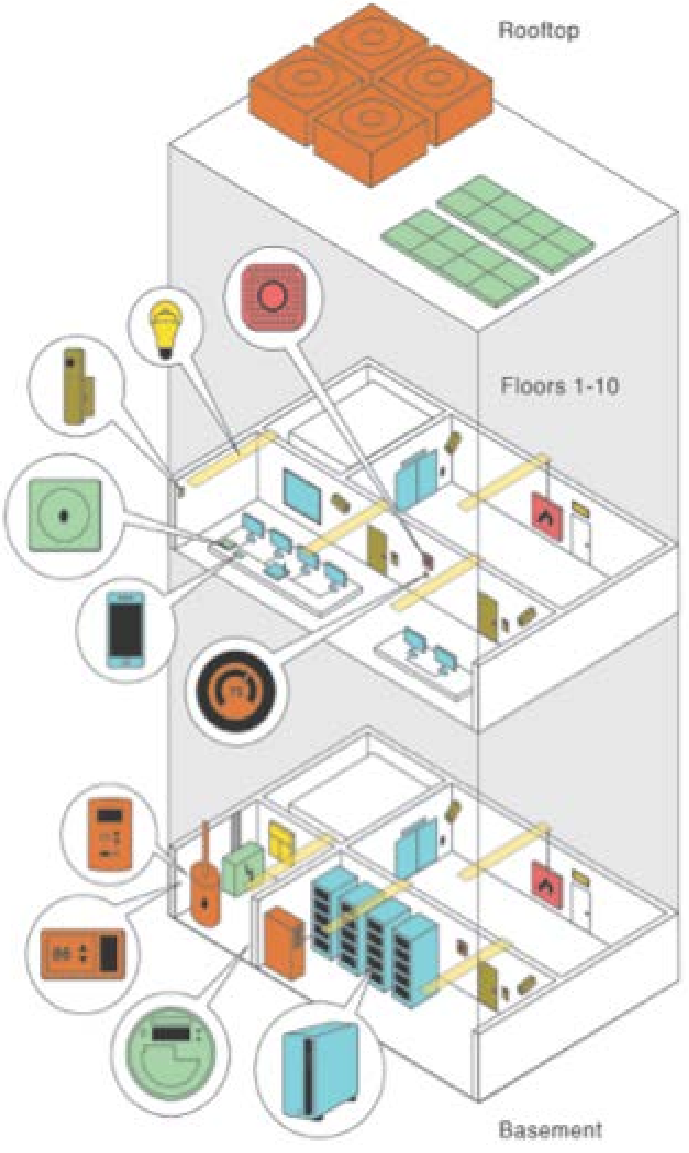
- 🔴 Smart Security Alarms (fire alarms, etc.)
- 🟢 Energy Management & BAS
- 🟤 Security, Monitoring, & Access
- 🟡 Smart Environment Control (lighting, etc.)
- 🔵 Mobility & Information Communication
- 🟠 HVAC

Vulnerabilities

- 🟠 🟤 🟡 🟢 🔴 Lack of inventory and identification of Critical Cyber Assets (CCA)
- Lack of IT & OT security roles and responsibilities
- 🔵 🟢 Lack of patch management
- 🟠 🔵 🟢 Lack of separation between IT and OT networks
- 🟠 🟤 🟡 🔴 Lack of physical and cyber access control
- 🔵 Lack of authentication and encryption of CCA
- 🟢 Lack of periodic threat vulnerability assessments, penetration tests & mitigation
- 🔵 🟢 🔴 Lack of cybersecurity training and security audits
- 🟤 🟢 Lack of redundancy
- 🔵 🟢 Poor password management policies
- 🔵 🟢 Default software and network configurations
- 🔵 🟢 Lack of data and configuration backups
- 🟠 🟤 🔵 🟡 🟢 🔴 Lack of response and recovery plans
- 🟤 🔵 🟢 🔴 Lack of secure communication protocols
- 🟤 🔵 🟢 Lack of a risk management strategy



Building Cybersecurity Mitigation Recommendations



- Implement network segregation
- Implement password management policies (strong passwords)
- Change default SSID. Hide SSID and MAC filtering (especially for residential)
- Implement firewalls and configuration policies
- Encrypt all means of data transfer/information communication
- Determine roles and responsibilities; estalish access control
- Provide cybersecurity awareness education and training to all building personnel
- Securely store and exchange control systems data to protect against data/privacy breaches
- Implement plans for asset and network redundancy
- Implement plans for asset transfers and backups
- Implement integrity checks for automation software and firmware
- Implement backup mechanism for sensitive information
- Run periodic vulnerability, continuity, and penetration tests
- Implement vulnerability management plan
- Authenticate, approve, and log remote maintenance of building assets
- Maintain and protect audit logs such as Firewall logs, network audits

DOE - Integrated Joint Cybersecurity Coordination Center (iJC3) Cyber-Physical Assessments

BUILDINGS CYBERSECURITY CAPABILITY MATURITY MODEL

KALI LINUX

"the quieter you become, the more you are able to hear"

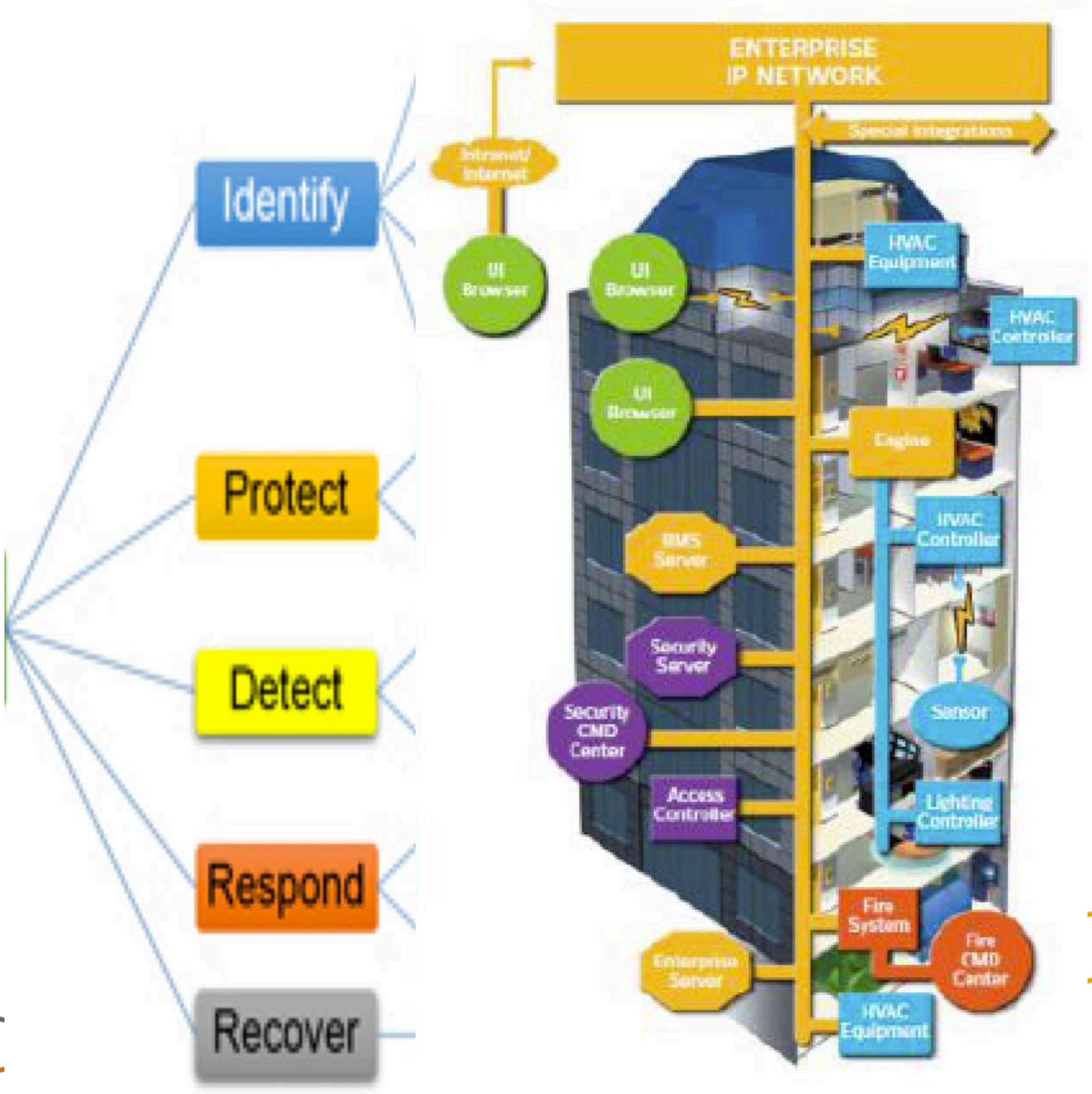
```
                    Boot menu

Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence              (check kali.org/prst)
Live USB Encrypted Persistence    (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options                                      >
```

How to Build a Low-Cost, Extended-Range RFID Skimmer

DOE-PNNL Buildings Cybersecurity Framework

DOE

Buildings Cybersecurity Framework



The Buildings Cybersecurity Framework will help identify, protect, detect, respond, recover and mitigate cyber-physical security threats to buildings

DOE-PNNL Buildings Cybersecurity Framework

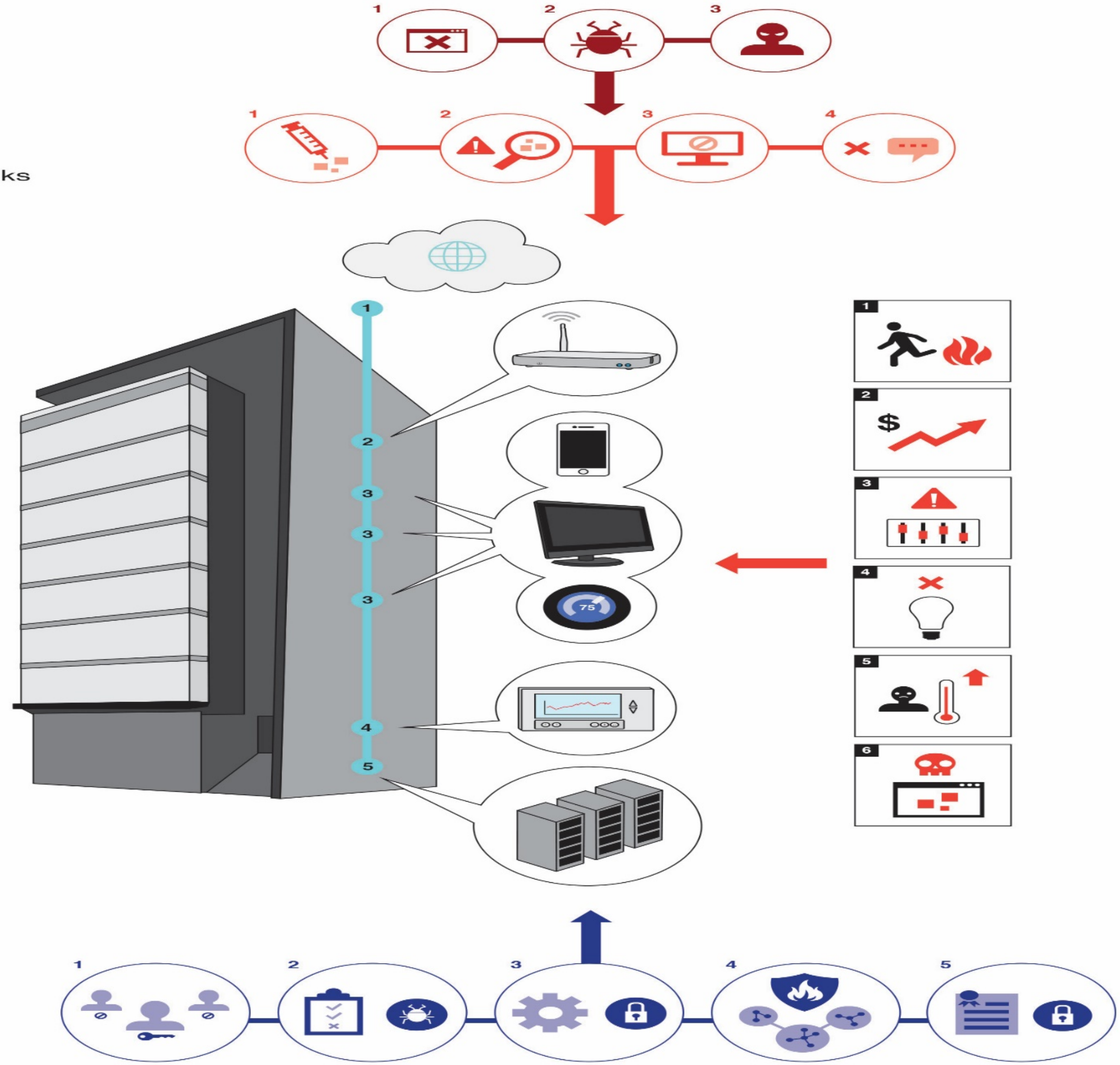
● **Threats**
1. Human Error
2. Malware
3. Attackers

● **Attacks**
1. Data injection attacks
2. Data integrity attacks
3. Denial of Service (DoS) attacks
4. Timing attacks

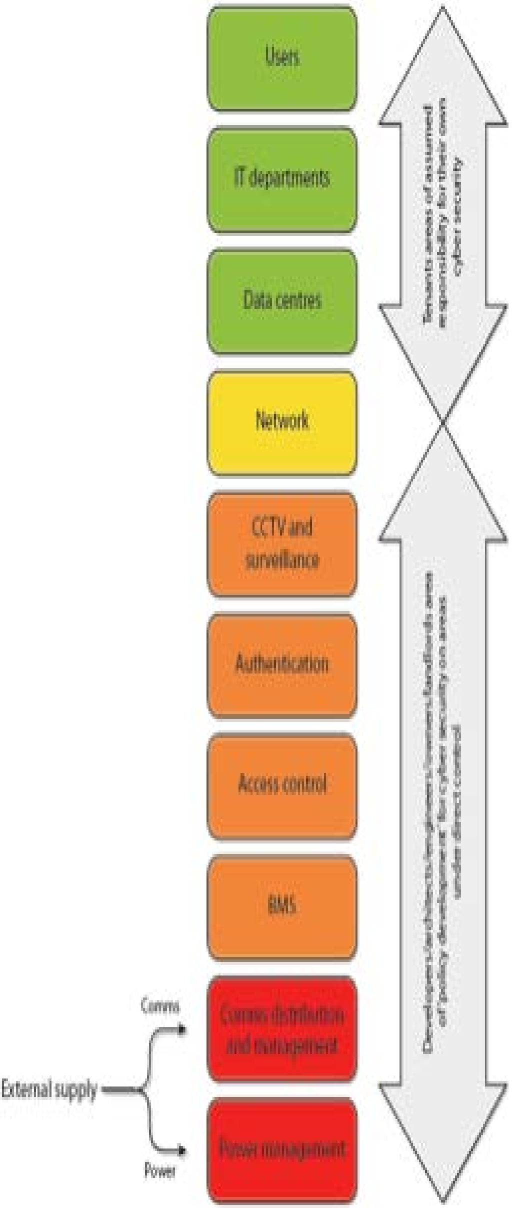
● **Building Connections**
1. Internet
2. Router
3. Networked devices
4. BAS controller
5. Data center

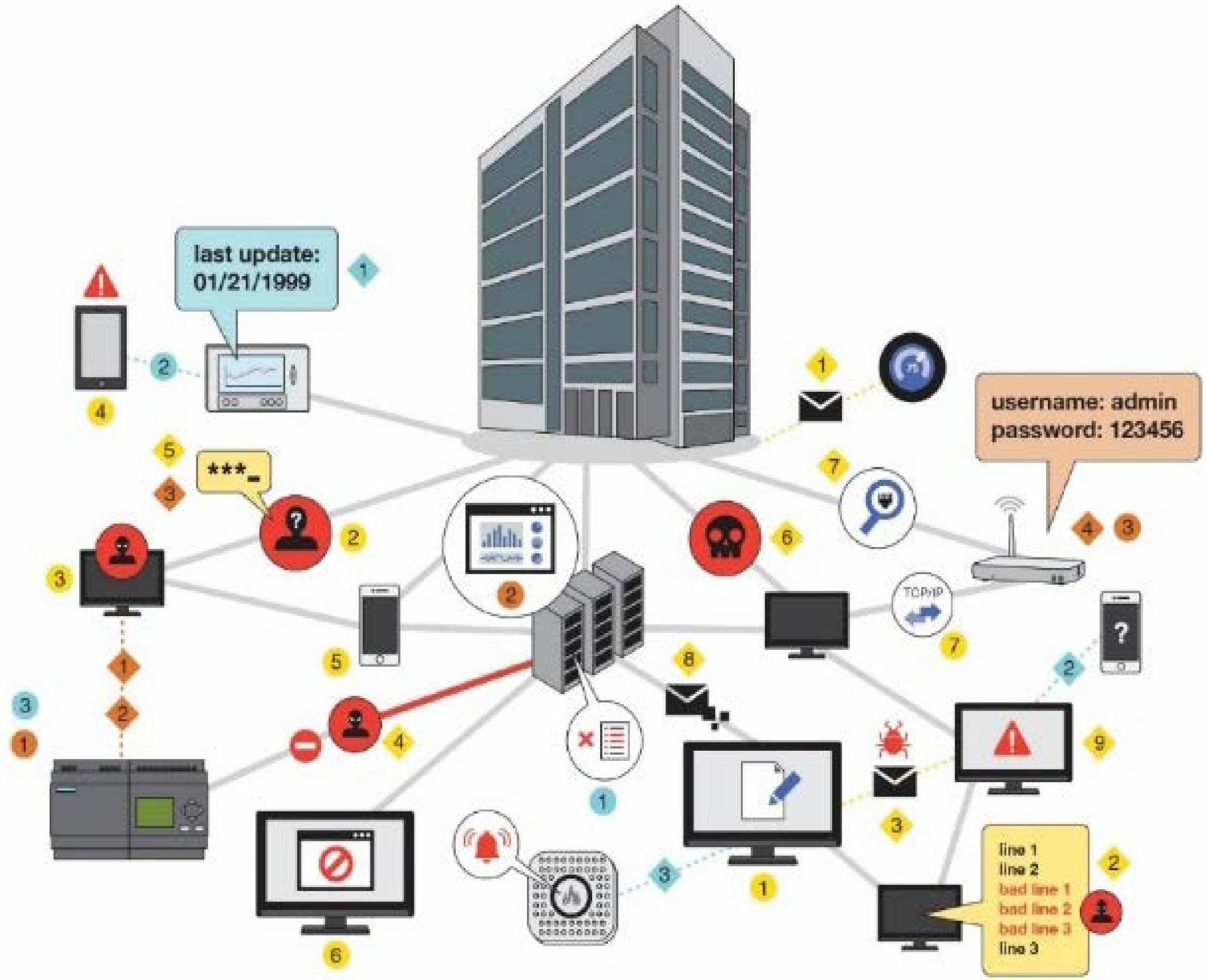
■ **Impacts**
1. Impact to life and occupant safety
2. Impact to operational economics
3. Impact to BAS components
4. Impact to BAS services
5. Impact to occupant activity and comfort
6. Impact to data and software

● **Critical Buildings Cybersecurity Control Schemes**
1. Access control
2. Vulnerability testing
3. Secure configuration of assets
4. Defense and protection of assets
5. Cybersecurity training and awareness

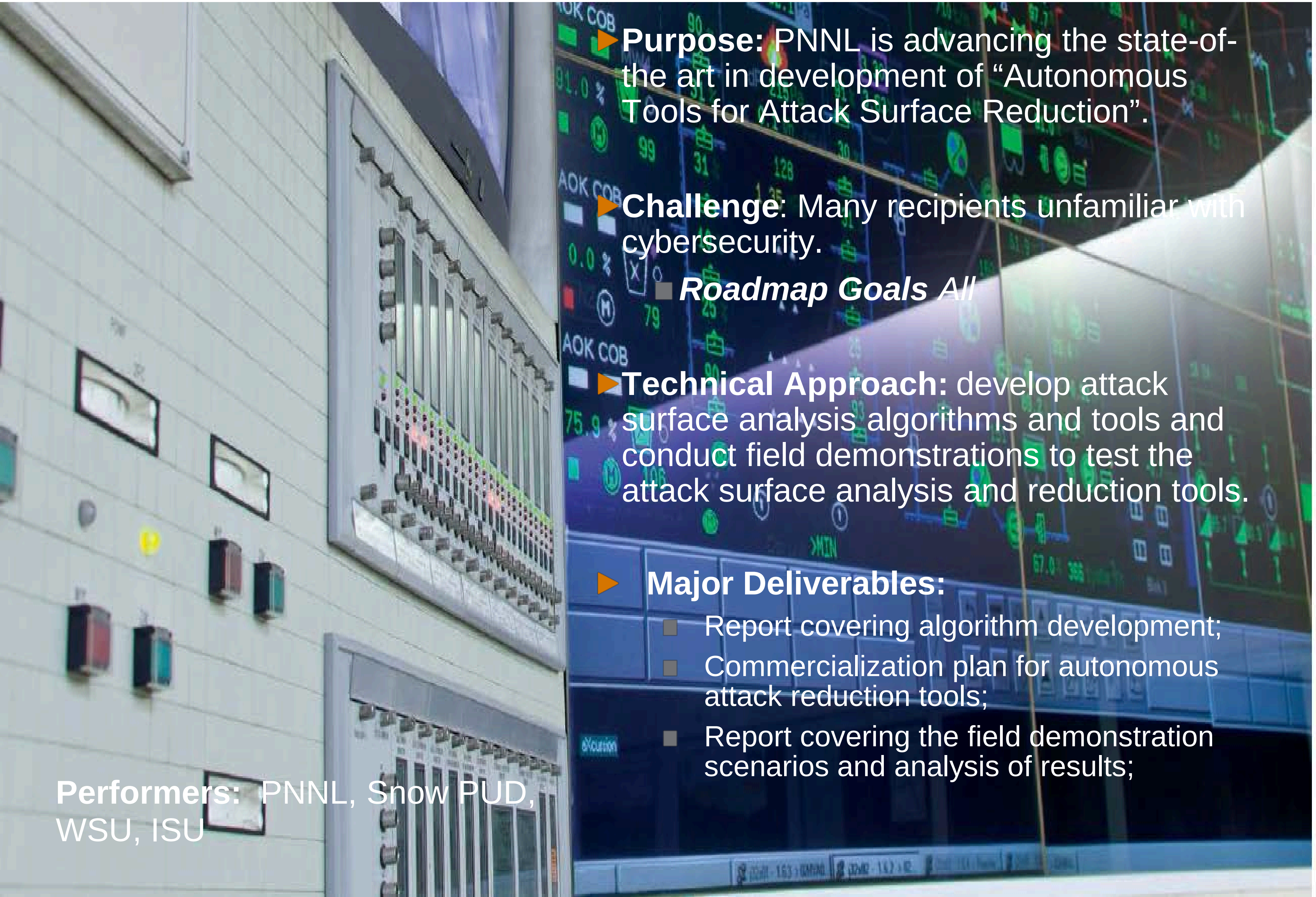


Training The Next Generation Buildings, Energy, IT and OT Security Manager


Users
IT departments
Data centres
Network
CCTV and surveillance
Authentication
Access control
BMS
Comms distribution and management
Power management
Comms
External supply
Power
Tenants areas of assumed responsibility for their own cyber security
Developers/architects/engineers/owners/landlords area of policy development for cyber security on areas under direct control



DOE-OE & PNNL Autonomous Tools for Attack Surface



- **Purpose:** PNNL is advancing the state-of-the art in development of “Autonomous Tools for Attack Surface Reduction”.

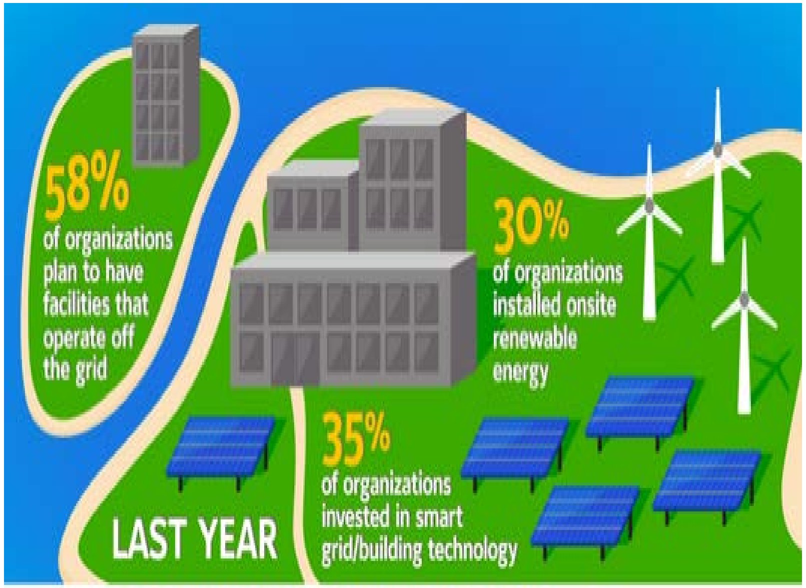
- **Challenge**: Many recipients unfamiliar with cybersecurity.
  - ***Roadmap Goals** All*

- **Technical Approach:** develop attack surface analysis algorithms and tools and conduct field demonstrations to test the attack surface analysis and reduction tools.

- **Major Deliverables:**
  - Report covering algorithm development;
  - Commercialization plan for autonomous attack reduction tools;
  - Report covering the field demonstration scenarios and analysis of results;

Performers: PNNL, Snow PUD, WSU, ISU

DOE OE & PNNL Integration of Renewable Energy Sources Securely with the Buildings and Electric Power


58%
of organizations plan to have facilities that operate off the grid
30%
of organizations installed onsite renewable energy
35%
of organizations invested in smart grid/building technology
LAST YEAR

- **Performers:** PNNL, UTRC, UICU

- **Purpose:** This project will deliver advanced attack detection and resiliency-enabling cybersecurity platform called INGRESS for behind-the-meter distributed energy resources that will be deployable within *legacy* and *emerging* energy system environments.

- **Challenges**: Lack of fidelity and security in buildings to grid deployment of distributed energy resources.

- **Major Deliverables:** Techniques to sense the health of the grid from the edge and also detect attacks emerging from the grid-edge devices
- A collection of attack-resilient techniques implemented in VOLTTRON

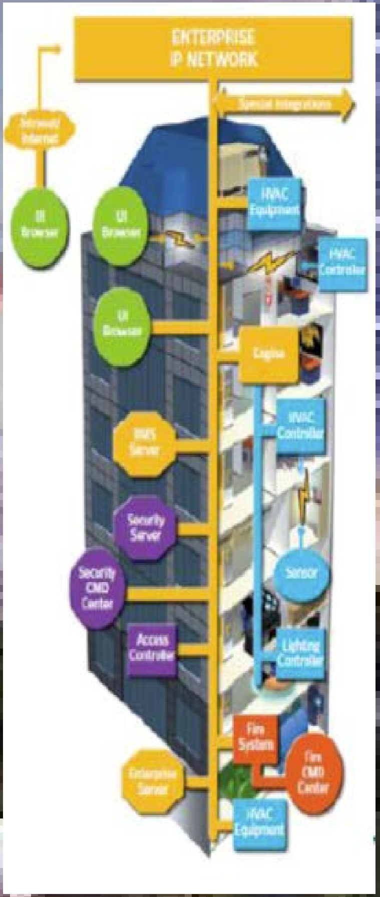
Cyber Secure - Facility Energy Decision System (CS-FEDS)

Challenges

Challenge 1: Cybersecurity solutions often times increase costs, reduce functionality and lack a clear value proposition.

Challenge 2: Networking and digitizing energy technology and controls can reduce costs, increase functionality and efficiency, but often times increases cyber vulnerabilities.

Challenge 3: A turn key tool to improve energy efficiency and cybersecurity does not exist



Proposed Solution

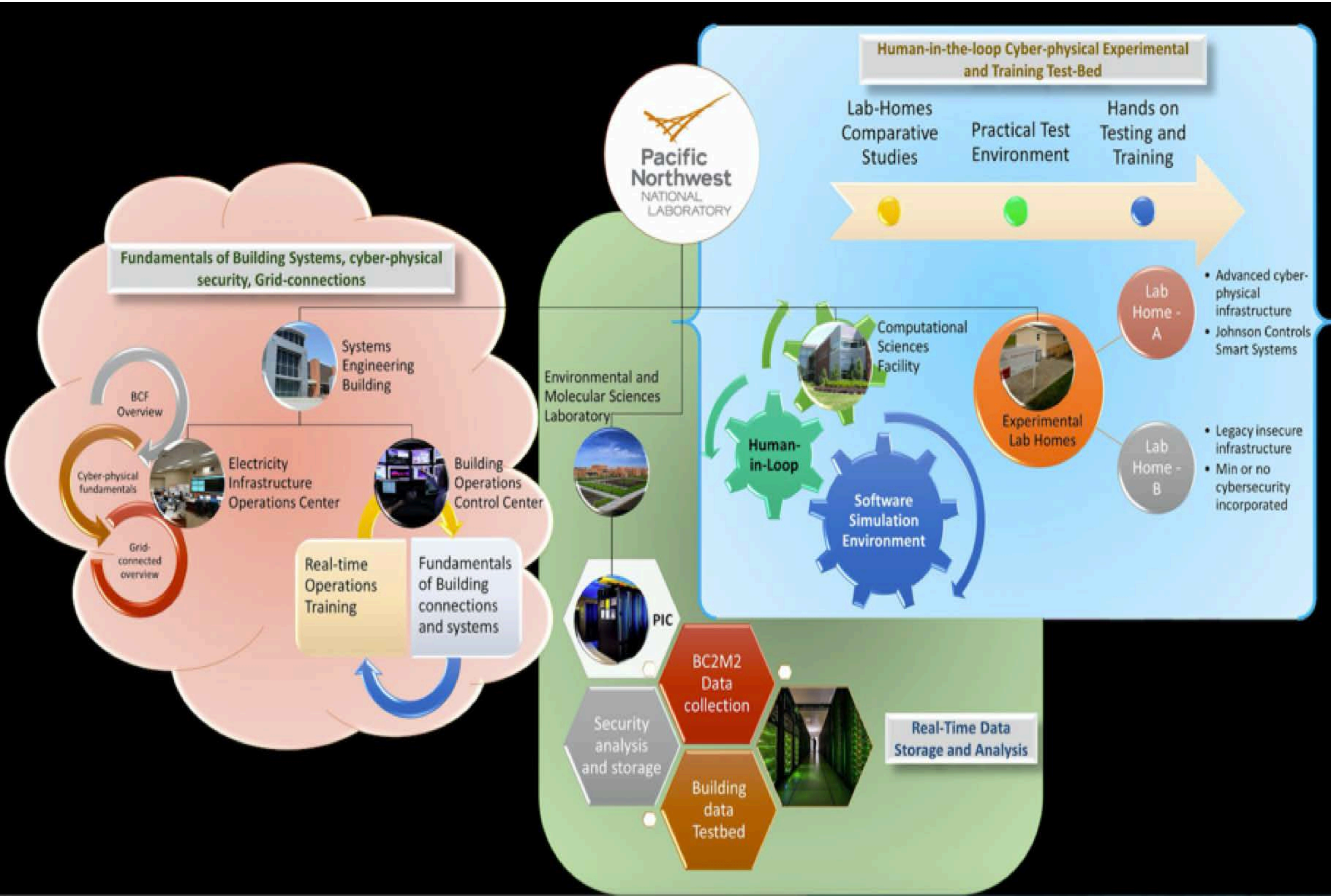
- PNNL have beta tested a tool called the Cyber Secure - Facility Energy Decision System (CS-FEDS) that could potentially help building owners reduce their energy consumption, while increasing their cybersecurity maturity and situational awareness.

Key Features

- Models energy and cost performance of heating, cooling, ventilation, lighting, motors, plug loads, building shell, and hot water systems, plus central plants and thermal loops.
- Models buildings systems interoperability and inventories critical cyber assets
-Identifies cybersecurity vulnerabilities in building automation systems

Turn-Key buildings cybersecurity and energy efficiency tool

Buildings-To-Grid Cybersecurity Testbed



Human-in-the-loop Cyber-physical Experimental and Training Test-Bed

Lab-Homes Comparative Studies

Practical Test Environment

Hands on Testing and Training

Pacific Northwest NATIONAL LABORATORY

Fundamentals of Building Systems, cyber-physical security, Grid-connections

Systems Engineering Building

BCF Overview

Cyber-physical fundamentals

Grid-connected overview

Electricity Infrastructure Operations Center

Building Operations Control Center

Real-time Operations Training

Fundamentals of Building connections and systems

Environmental and Molecular Sciences Laboratory

PIC

BC2M2 Data collection

Security analysis and storage

Building data Testbed

Real-Time Data Storage and Analysis

Computational Sciences Facility

Human-in-Loop

Software Simulation Environment

Experimental Lab Homes

Lab Home - A

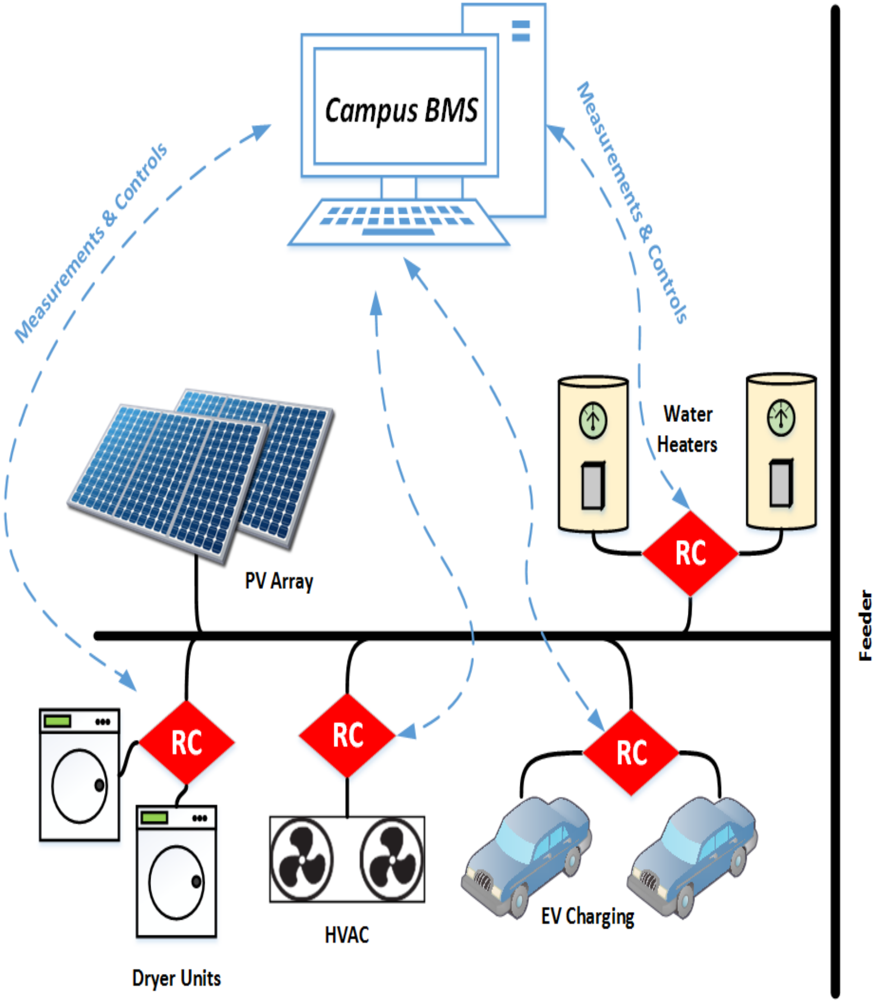
- Advanced cyber-physical infrastructure
- Johnson Controls Smart Systems

Lab Home - B

- Legacy insecure infrastructure
- Min or no cybersecurity incorporated

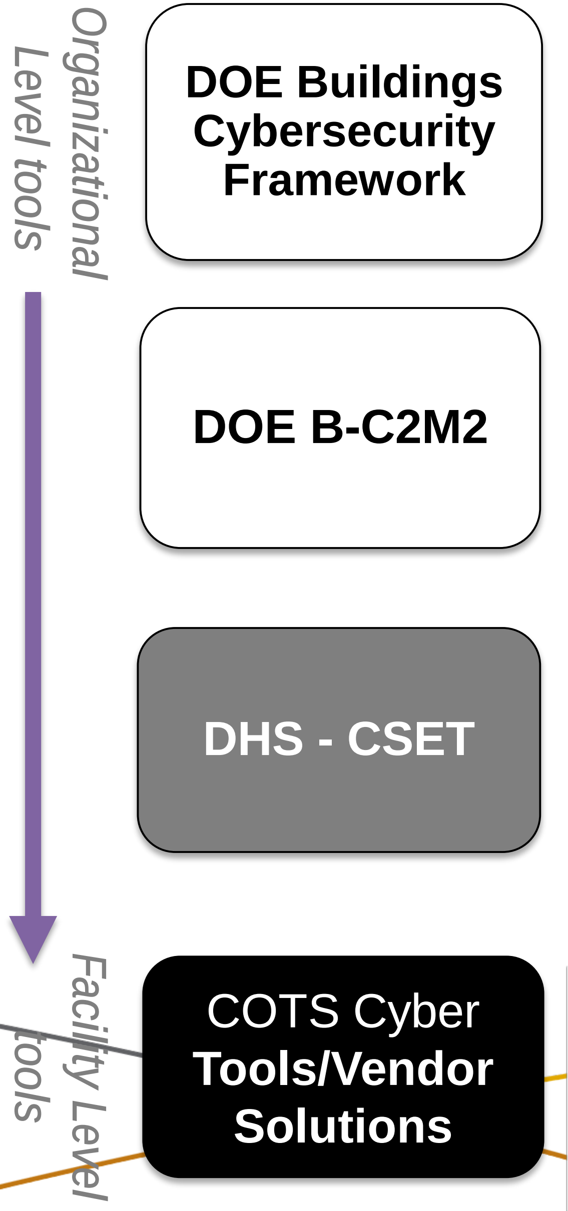
Resilient Controllers for Campus BMS

- Demand Side Management
  - Schedulable/controllable loads
  - Distributed energy resources
  - Transactive energy schemes
  - Utility contracts
- Increasing cyber threats
  - Vulnerable, insecure controllers
- Cyber attack impacts
  - Safety (Buildings/Occupants)
  - Property damage (Equipment)
  - Operational costs (Campus)
  - Energy security (Campus/Utility)



Need: Resilient Controllers for schedulable loads in a campus to detect and mitigate cyber attacks.

Buildings Cybersecurity Training – From Procurement to Policies, Systems to Implementation



DOE Buildings Cybersecurity Framework

Will provide an **actionable framework for establishing building specific cybersecurity policies and procedures**

DOE B-C2M2

Will provide **high level baseline and guidance for developing cybersecurity situational awareness for buildings**

- *Adapted from ES-C2M2 (e.g., utilities)*

DHS - CSET

Helps **assess the policies that are in place and the resources strengths as they relate to available industry standards**

- *Evaluates organization’s ICS and IT network security posture (not buildings specific)*

COTS Cyber **Tools/Vendor Solutions**

Commercial off the shelf technologies or scanning tools that map specific critical controls & technology solutions

- *Risk: scanning legacy buildings controls often causes them to crash because legacy systems didn’t contemplate cyber or IoT*

Contact Info

Michael Mylrea
Manager, Cybersecurity & Energy Technology
Pacific Northwest National Lab

michael.mylrea@pnnl.gov

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*