U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CISA
CYBER+INFRASTRUCTURE

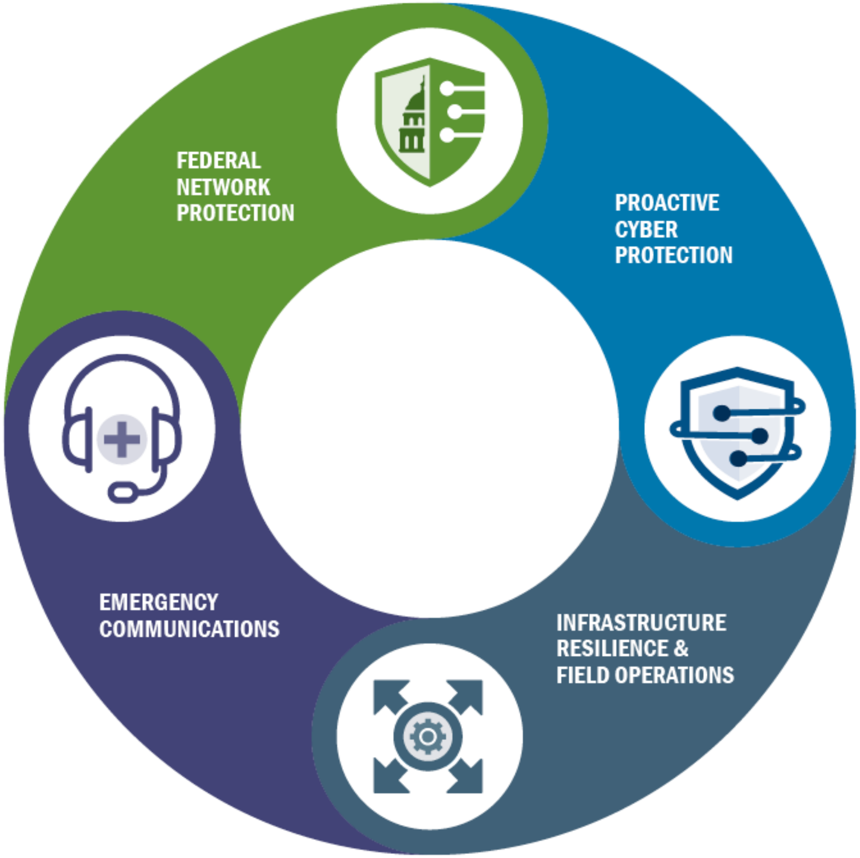
Klint Walker

Cyber Security Advisor, Region IV

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

The Nation’s Risk Managers

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure


FEDERAL NETWORK PROTECTION
PROACTIVE CYBER PROTECTION
INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS
EMERGENCY COMMUNICATIONS

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

FEDERAL NETWORK PROTECTION

PROACTIVE CYBER PROTECTION

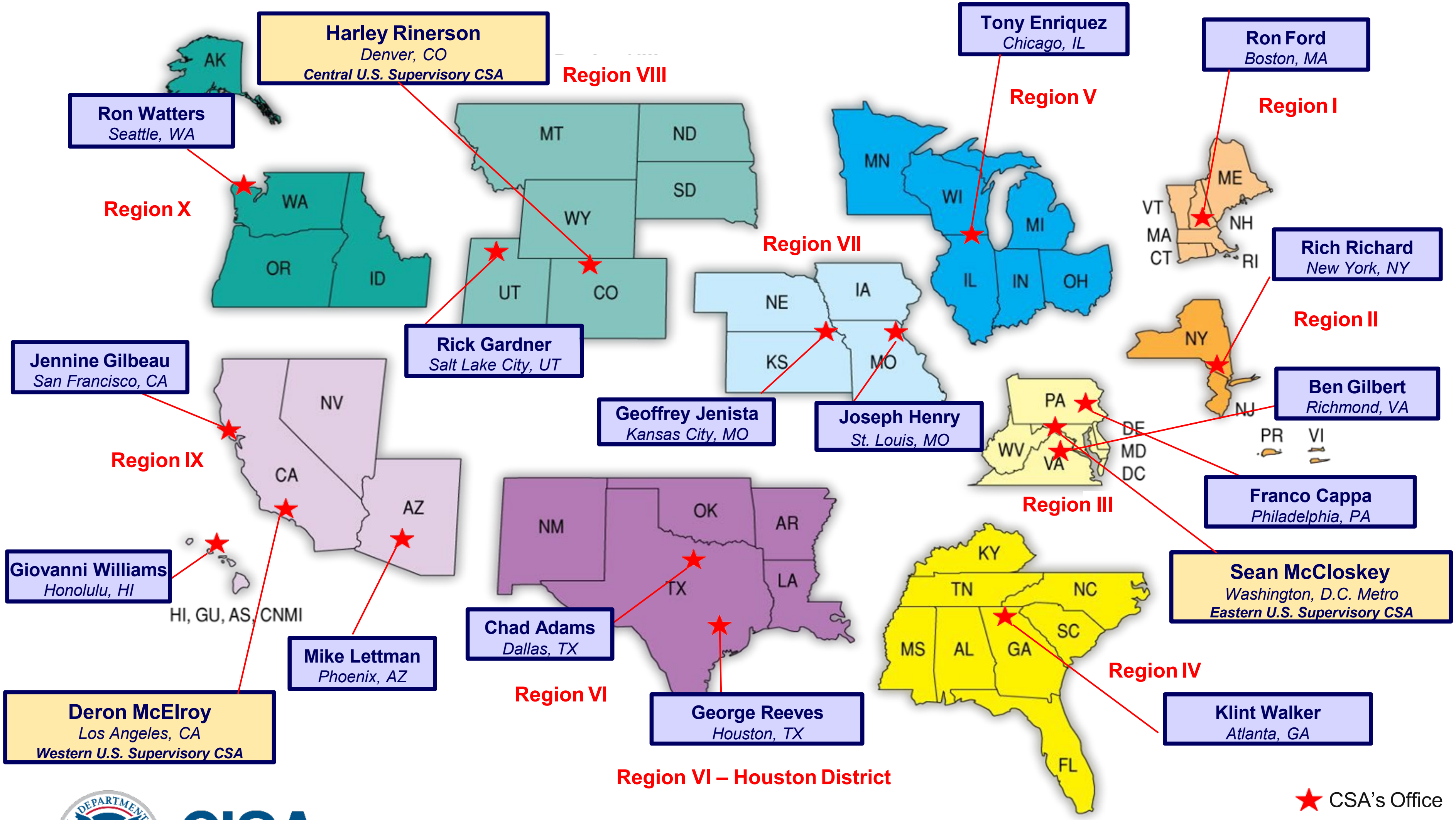
INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS

EMERGENCY COMMUNICATIONS

16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

CHEMICAL	DHS (CISA)
COMMERCIAL FACILITIES	DHS (CISA)
COMMUNICATIONS	DHS (CISA)
CRITICAL MANUFACTURING	DHS (CISA)
DAMS	DHS (CISA)
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	DHS (CISA)
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & DHS (FPS)
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	DHS (CISA)
NUCLEAR REACTORS, MATERIALS AND WASTE	DHS (CISA)
TRANSPORTATIONS SYSTEMS	(TSA & USCG)
WATER	EPA

CSA Deployed Personnel



Harley Rinerson
Denver, CO
Central U.S. Supervisory CSA

Ron Watters
Seattle, WA

Rick Gardner
Salt Lake City, UT

Jennine Gilbeau
San Francisco, CA

Giovanni Williams
Honolulu, HI

Mike Lettman
Phoenix, AZ

Deron McElroy
Los Angeles, CA
Western U.S. Supervisory CSA

Geoffrey Jenista
Kansas City, MO

Joseph Henry
St. Louis, MO

Chad Adams
Dallas, TX

George Reeves
Houston, TX

Tony Enriquez
Chicago, IL

Ron Ford
Boston, MA

Rich Richard
New York, NY

Ben Gilbert
Richmond, VA

Franco Cappa
Philadelphia, PA

Sean McCloskey
Washington, D.C. Metro
Eastern U.S. Supervisory CSA

Klint Walker
Atlanta, GA

★ CSA's Office

CSA Program Mission

To provide direct coordination, outreach, and regional support in order to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's Critical Infrastructure and Key Resources (CIKR) and State, Local, Territorial, and Tribal (SLTT) governments.

Cyber Security Advisor (CSA) Program in recognition that a regional and national focused cyber security presence is essential to protect critical infrastructure.

CSAs represent a front line approach and promote resilience of key cyber infrastructures throughout the U.S. and its territories.

CSA Program Activities

CSAs support four key DHS goals:

- Cyber Preparedness
- Risk Mitigation
- Incident & Information Coordination
- Cyber Policy Promotion & Situational Awareness

CSAs facilitate three assessments:

- Cyber Resilience Reviews (CRR)
- Cyber Infrastructure Surveys (C-IST)
- External Dependency Reviews (EDM)

CSAs participate in local / regional cyber working groups, mostly organized by Federal and state partners

Presidential Policy Directive 41 – Concurrent Lines of Effort

- Threat Response
  - Threat response activities include conducting appropriate law enforcement and national security investigative activities; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.
- Asset Response
  - Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery.
- Intelligence Support
  - Intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.

Today’s Risk Landscape

America remains at risk from a variety of threats:

ACTS OF TERRORISM

CYBER ATTACKS

EXTREME WEATHER

PANDEMICS

ACCIDENTS OR TECHNICAL FAILURES

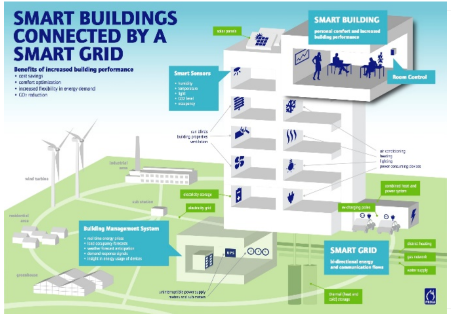
Cyberspace: Foundational to Our World

- Automation, technology, and network communications have become increasingly essential to our daily lives.
- The amount of information and data stored electronically has grown.
- There is a vast interconnectedness of relationships and dependencies, for example
  - government – private sector – international
  - third-party vendors
  - linkages within organizations
- As a result, the country is dependent on the cyber resilience of its critical infrastructure, such as, the power grid, banking and financial systems, and telecommunications

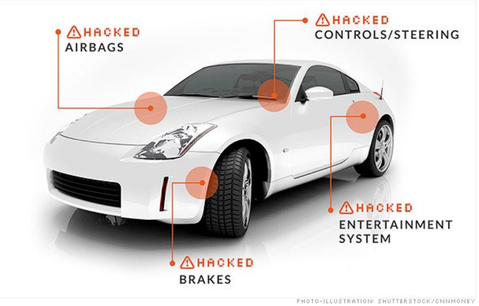
Cyber Security is Critical

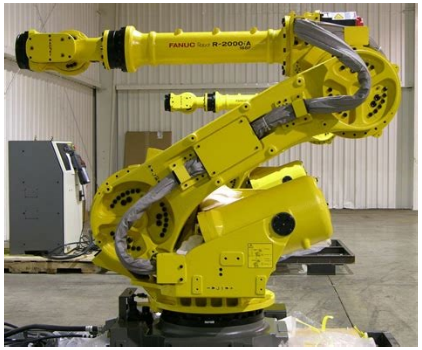
- Smart cars, grids, medical devices, manufacturing, homes, buildings, smart everything!
- We bet our lives on these systems
  - cyber security ⇔ physical safety!
- Yet, much of CPS are “cobbled together from stuff found on the Web”!
- Who minds the shop?

Our buildings


SMART BUILDINGS CONNECTED BY A SMART GRID
SMART BUILDING
Smart Sensors
Room Control
Building Management System
SMART GRID

Our transport


HACKED AIRBAGS
HACKED CONTROLS/STEERING
HACKED ENTERTAINMENT SYSTEM
HACKED BRAKES
PHOTO-ILLUSTRATION: SHUTTERSTOCK/CNNMONEY



Our Production

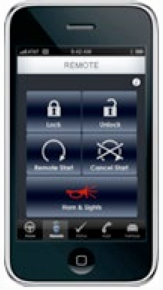
Our health

Homeland Security

Vehicle Security – Many things to go wrong

200M lines of code in a modern vehicle!

- **Telematics**
  - Remote control (locks, start)
  - Remote diagnostics
  - Remote repair (updates)



- **Driver support**
  - Navigation
  - Collision warning/avoidance
  - Augmented vision

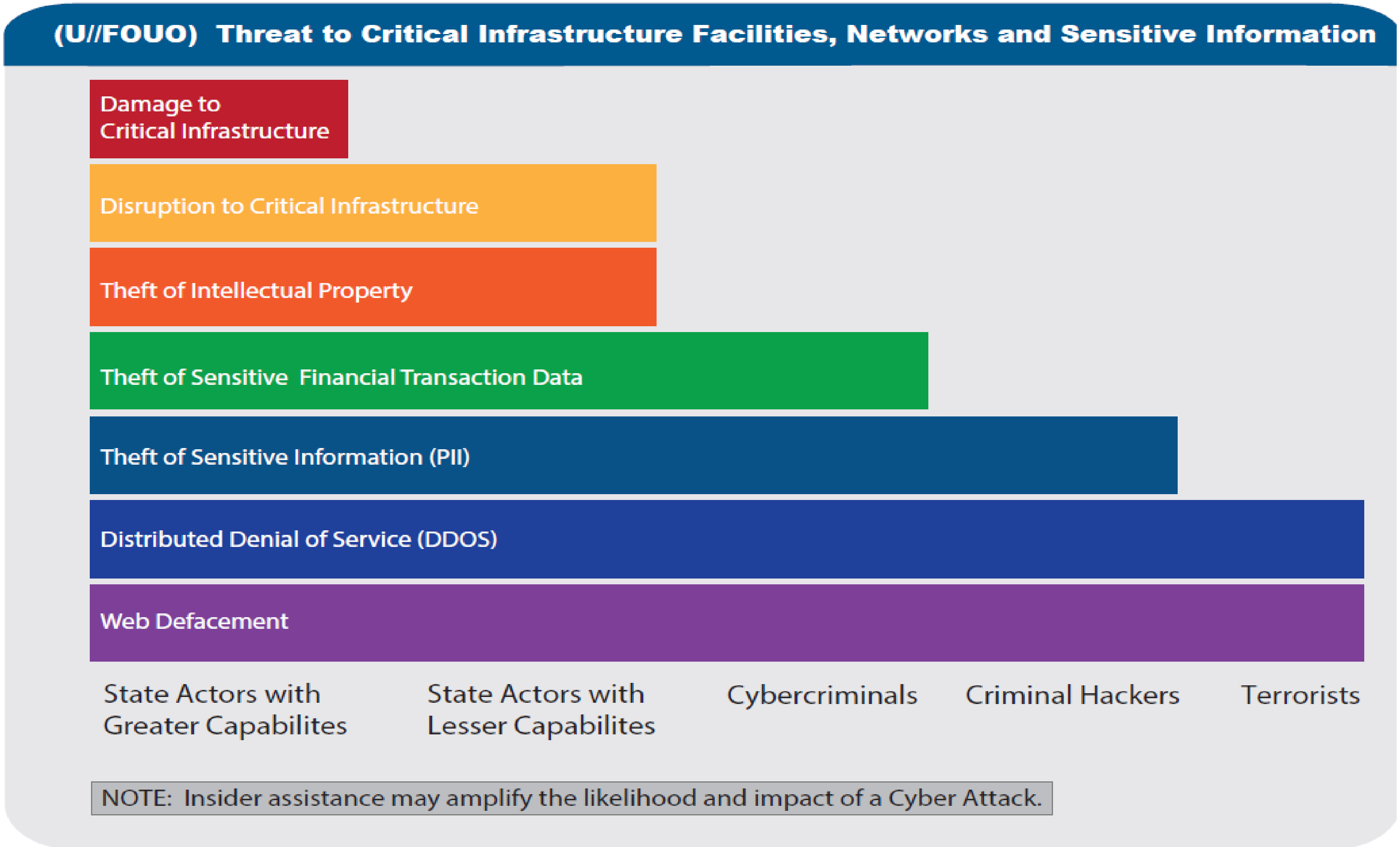
- **System automation**
  - Dynamic EV charging
  - Computer control of engine, brakes, etc.

- **Content and communication**
  - Voice and data
  - Information and entertainment

A Growing Challenge

- **Scale**: The number of cyber attacks has never been greater.
- **Sophistication** : Cyber attacks are increasing in complexity.
- **Trends**: Attackers are increasing their advantage.
- **Attack Surface**: Growing volumes of data = more targets.

Threat Landscape



(U//FOUO) Threat to Critical Infrastructure Facilities, Networks and Sensitive Information

Damage to Critical Infrastructure

Disruption to Critical Infrastructure

Theft of Intellectual Property

Theft of Sensitive Financial Transaction Data

Theft of Sensitive Information (PII)

Distributed Denial of Service (DDOS)

Web Defacement

State Actors with Greater Capabilites

State Actors with Lesser Capabilites

Cybercriminals

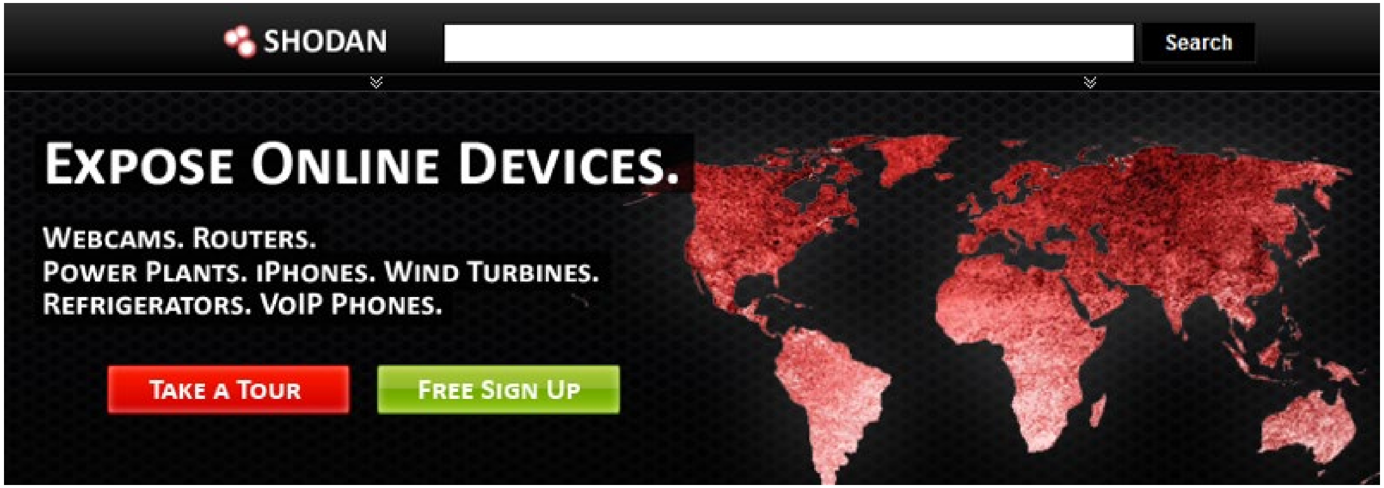
Criminal Hackers

Terrorists

NOTE: Insider assistance may amplify the likelihood and impact of a Cyber Attack.

Homeland Security

ShodanHQ



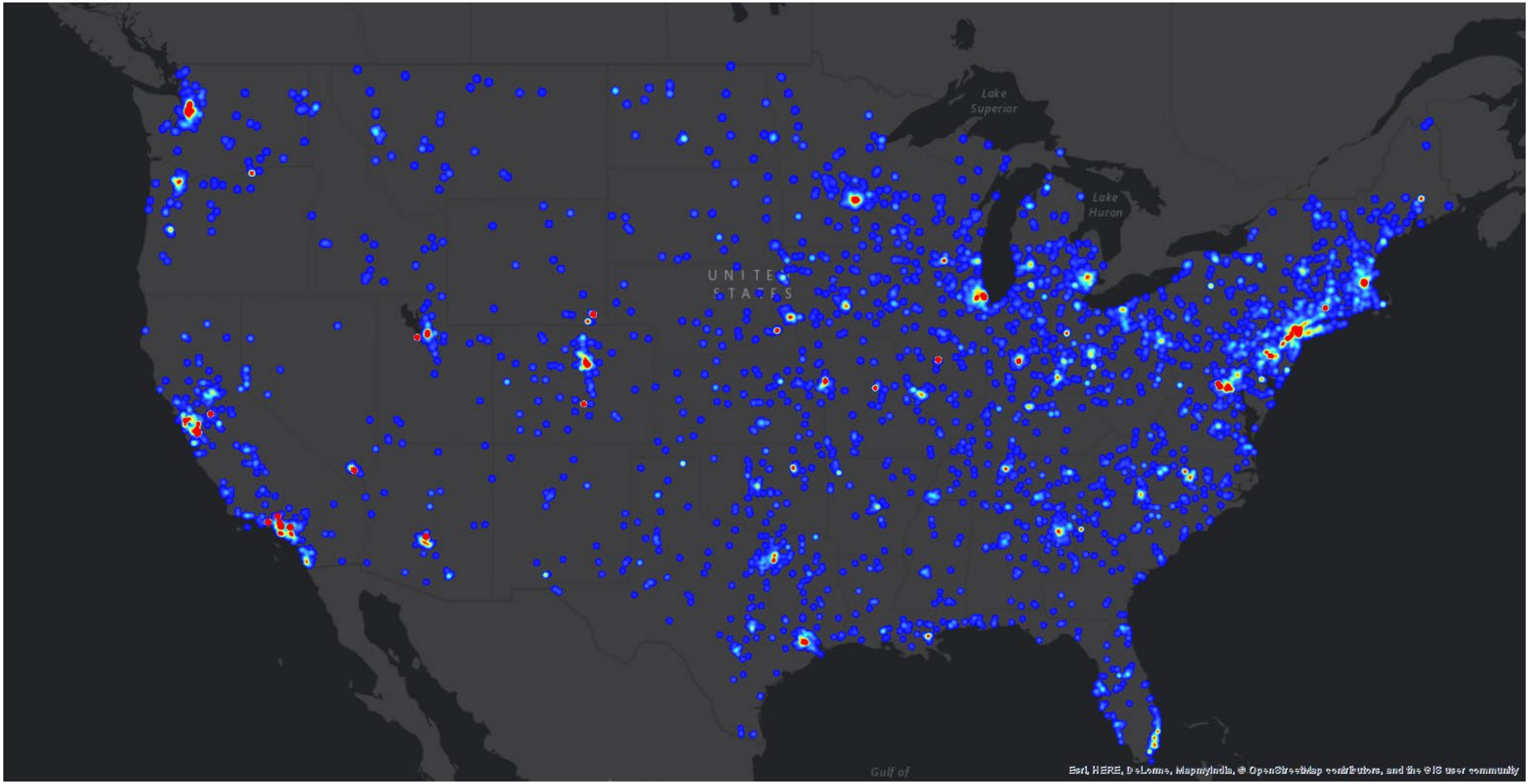
EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

- ShodanHQ is the first search engine designed to search for computers and devices.
- ***Recommendation: Run a search using your network IP range to identify or validate: devices, misconfigurations, location, services, HW/SW versions, etc.***

- ShodanHQ has identified:
  - **~500,000** devices connected to the internet
  - **98,415** were located in the U.S.
  - **7,257** were associated with Industrial Control Systems

How many ICS devices are connected?



Esri, HERE, DeLorme, MapmyIndia, © OpenStreetMap contributors, and the GIS user community

Homeland Security

IT vs. OT

SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
ANTIVIRUS & MOBILE CODE COUNTER-MEASURES	Common & widely used	**Can be difficult to deploy**
SUPPORT TECHNOLOGY LIFETIME	3 to 5 years	**Up to 40+ years**
OUTSOURCING	Common/widely used	**Rarely used (vendor only)**
APPLICATION OF PATCHES	Regular/ scheduled	**Slow (vendor specific, compliance testing required)**
CHANGE MANAGEMENT	Regular/ scheduled	**Legacy based – unsuitable for modern security**
TIME CRITICAL CONTENT	Delays are usually accepted	**Critical due to safety**
AVAILABILITY	Delays are usually accepted	**24 x 7 x 365 x forever (Integrity also critical)**
SECURITY AWARENESS	Good in both private and public sector	**Generally poor inside the control zone**
SECURITY TESTING/ AUDIT	Scheduled and mandated	**Occasional testing for outages / audit for event recreation**
PHYSICAL SECURITY	Secure	**Traditionally good**

Cyber Supply Chain

Cybersecurity in the supply chain cannot be viewed as an IT only problem.

- Cyber supply chain risks include:
  - sourcing,
  - vendor management,
  - supply chain continuity and quality,
  - transportation security
  - and many other functions across the enterprise
- Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem.
- Require a coordinated effort to address.

Cyber Supply Chain Attack Examples

- Target (2014) – HVAC security
- Equifax – 3rd Party Software flaw
- Verizon – Flawed Analytic software
- Paradise Papers – Data hacked from legal firms
- Domino’s Pizza (Australia) – former 3rd party database hacked

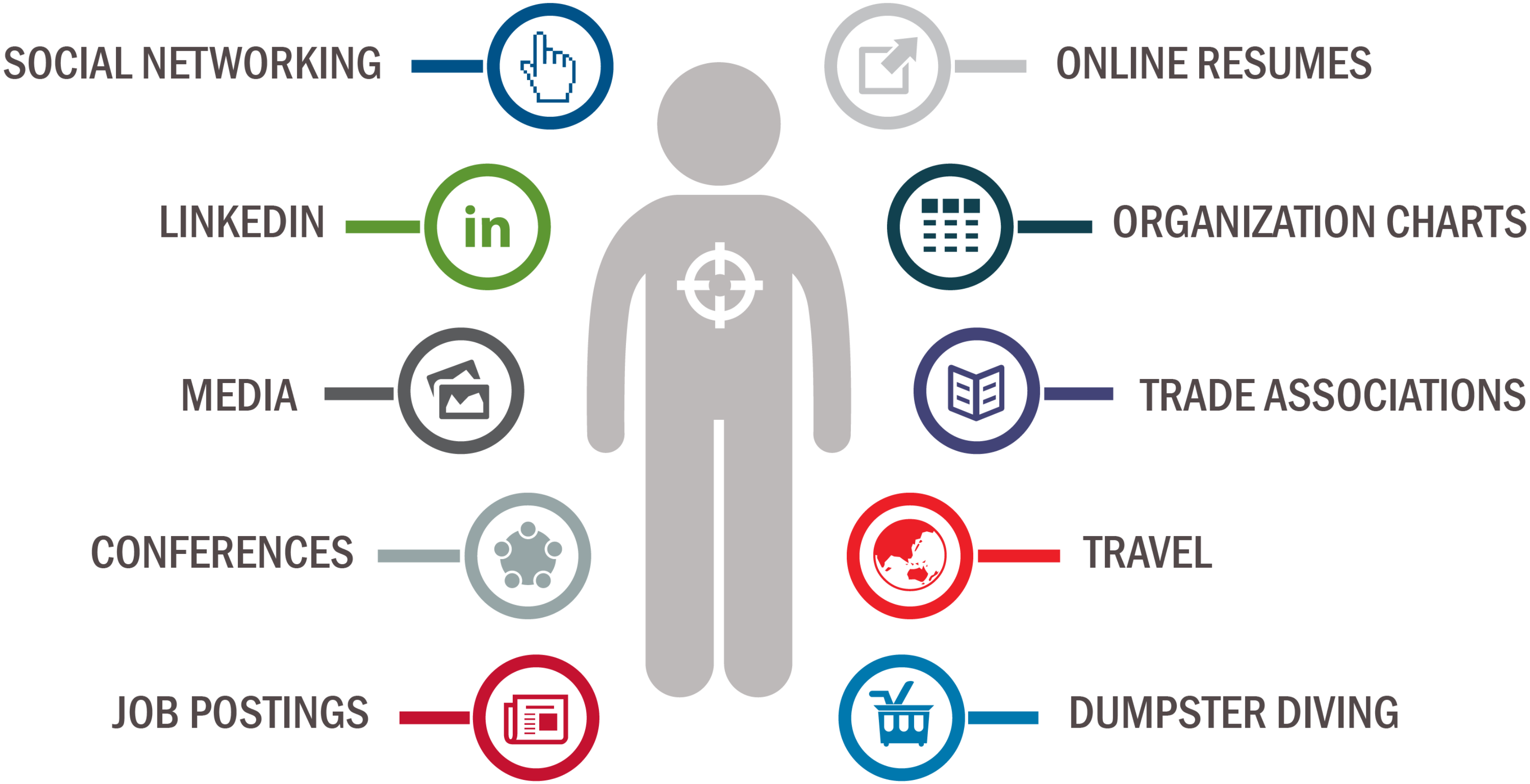
In a recent poll over 50 percent of organizations have had a breach that was caused by one of their vendors

Supply Chain Attacks Spiked 78 Percent in 2018, Cyber Researchers Found

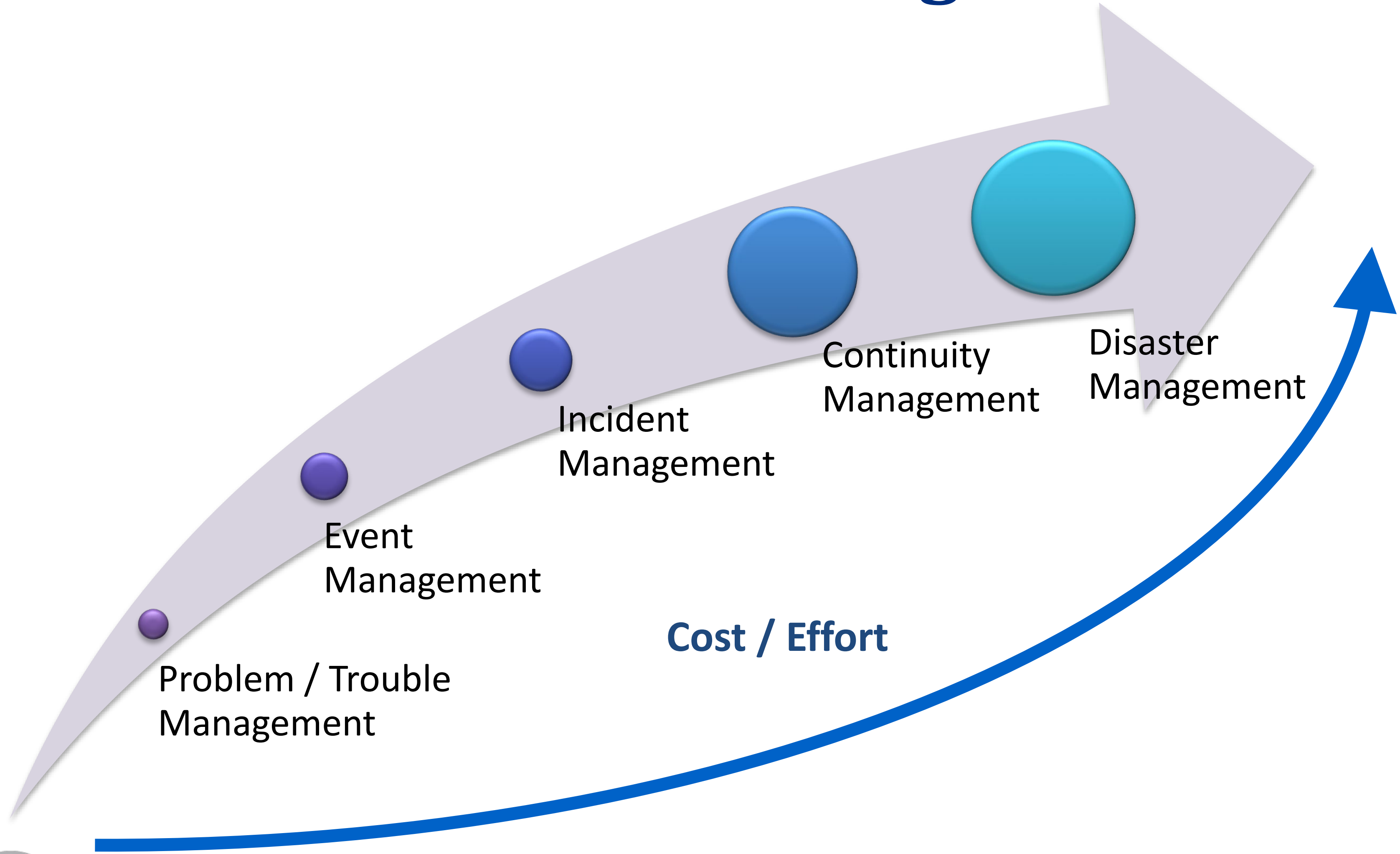
Cyber Supply Chain Threats

1. **Software service providers and outside contractors**
   - exploitation of smaller, typically less-secure companies who have access to or credentials for the networks of larger corporations
2. **Mergers and acquisitions**
   - Inheriting the (lack of) security for smaller companies
3. **Physical components**
   - hidden “backdoors” embedded in software or hardware
4. **Network services**
   - Do you know the route your digital traffic takes from one point to the next?
5. **IOT (internet of things)**
   - prioritize time-to-market over security

How Are You Targeted by Foreign Intel?



Operational Planning for Cyber Security Events, Attacks, and Contingencies



Problem / Trouble Management

Event Management

Incident Management

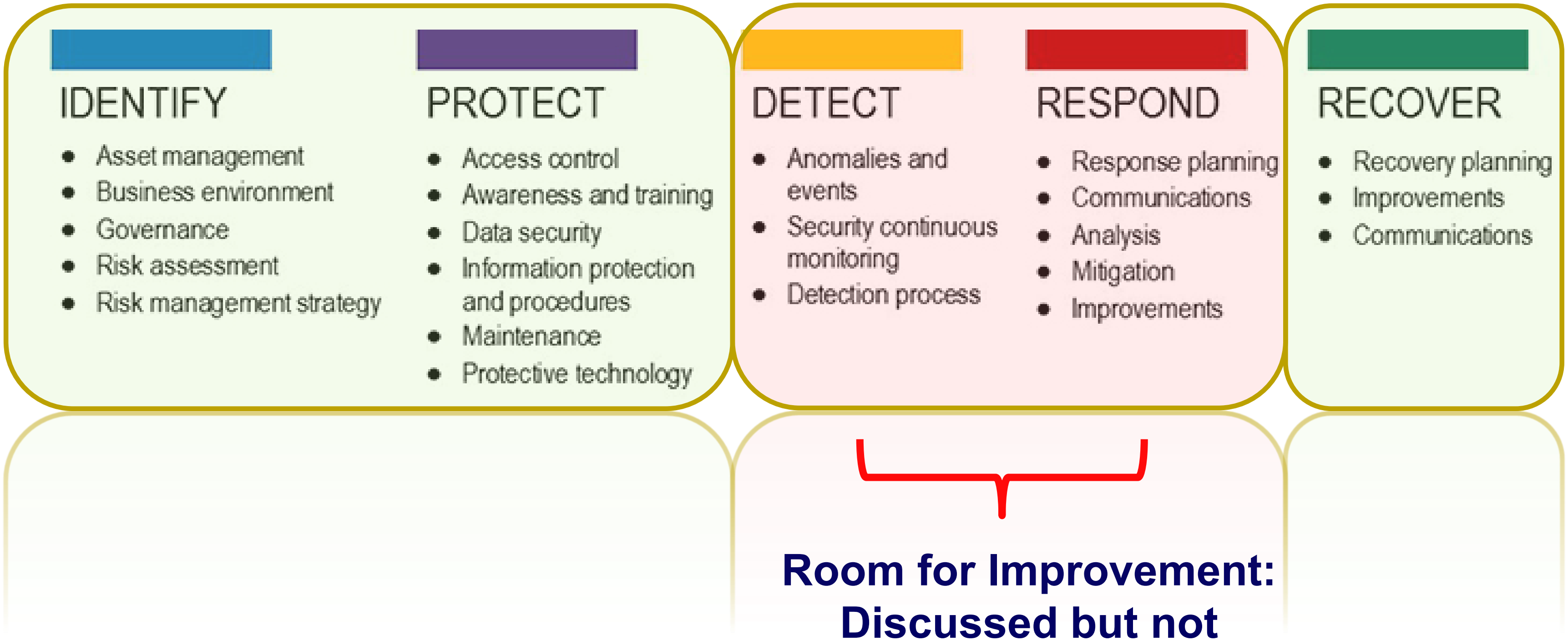
Continuity Management

Disaster Management

Cost / Effort

CSF and the State of Cybersecurity Management

Status Quo: Practiced, Planned, & Resourced



IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT

- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT

- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND

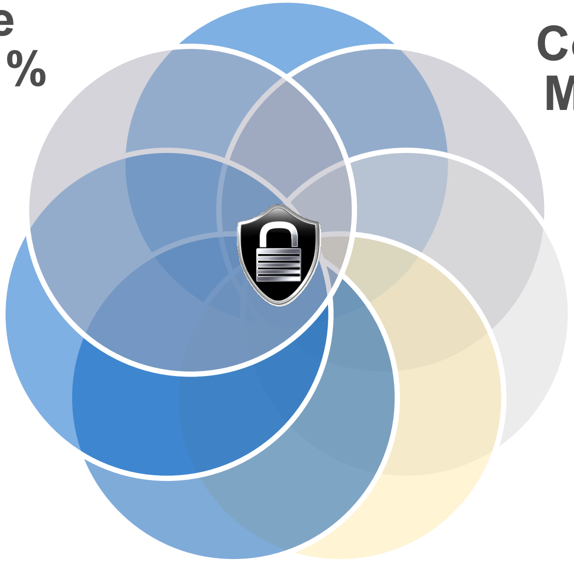
- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recovery planning
- Improvements
- Communications

Room for Improvement: Discussed but not Deliberate, Less Practiced, Planned, & Resourced

Incident Response Root Cause Analysis*



Implement Application Whitelisting – 38%

Ensure Proper Configuration/Patch Management – 29%

Reduce your Attack Surface Area – 17%

Build a Defendable Environment – 9%

Manage Authentication – 4%

Monitor and Respond – 2%

Implement Secure Remote Access – 1%

*Based on FY14-15 ICS-CERT Incident Response Data

A Wide Range of Offerings for Critical Infrastructure

- National Cybersecurity and Communications Integration Center (NCCIC)
  - US-CERT Operations Center
    - **Remote / On-Site Assistance**
    - **Malware Analysis**
    - **Incident Response Teams**
  - ICS-CERT Operations Center
    - **ICS-CERT Malware Lab**
    - **Incident Response Teams**
  - Cyber Exercise Program

- Cyber Security Advisors
- Protective Security Advisors

- Preparedness Activities
  - **National Cyber Awareness System**
  - **Vulnerability Notes Database**
  - **Security Publications**
  - **Technical Threat Indicators**
  - **Cybersecurity Training**
  - **Information Products and Recommended Practices**
- Control Systems Evaluations
  - **Cyber Security Evaluation Tool**
  - **ICS Design Architecture Reviews / Network Architecture Analysis**
- Other Cyber Security Evaluations
  - **Cyber Resilience Review**
  - **Cyber Infrastructure Survey**
  - **Cyber Hygiene service**
  - **Risk and Vulnerability Assessment (aka "Pen" Test)**

Homeland Security

Sampling of Cybersecurity Offerings

- **Preparedness Activities**
  - Information / Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber Exercises and "Playbooks"
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices
  - Cybersecurity Evaluations
    - Cyber Resilience Reviews (CRR™)
    - Cyber Infrastructure Surveys
    - Phishing Campaign Assessment
    - Vulnerability Scanning
    - Risk and Vulnerability Assessments (aka "Pen" Tests)
    - External Dependency Management Reviews
    - Cyber Security Evaluation Tool (CSET™)
    - Validated Architecture Design Review (VADR)

- **Response Assistance**
  - Remote / On-Site Assistance
  - Malware Analysis
  - Hunt and Incident Response Teams
  - Incident Coordination

- **Cybersecurity Advisors**
  - Assessments
  - Working group collaboration
  - Best Practices private-public
  - Incident assistance coordination

- **Protective Security Advisors**
  - Assessments
  - Incident liaisons between government and private sector
  - Support for National Special Security Events

Range of Cybersecurity Assessments

STRATEGIC
(C-Suite Level)

- Cyber Resilience Review (Strategic)--------------------------
- External Dependencies Management (Strategic)----------
- Cyber Infrastructure Survey (Strategic)----------------------
- Cybersecurity Evaluations Tool Strategic/Technical)-----
- Phishing Campaign Assessment (EVERYONE)-----------
- Vulnerability Scanning / Hygiene (Technical)---------------
- Validated Architecture Design Review (Technical)--------
- Risk and Vulnerability Assessment (Technical)-------------

TECHNICAL
(Network-Administrator Level)

VULNERABILITY SCANNING

Vulnerability Scanning

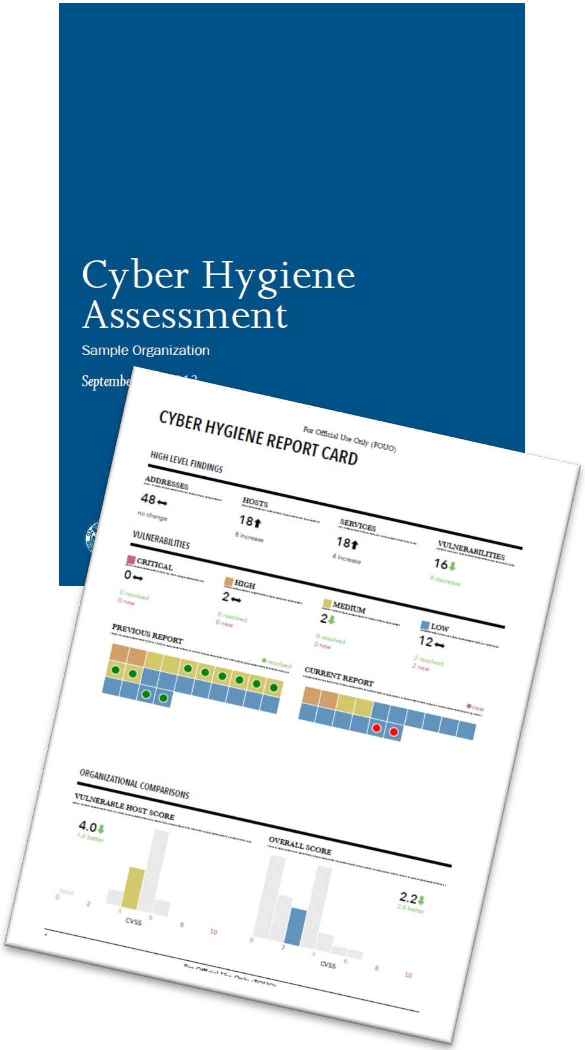
Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

Delivery: Online by CISA

Benefits:

- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities

  - **Network Vulnerability & Configuration Scanning**
    - Identify network vulnerabilities and weakness



Cyber Hygiene Assessment

Sample Organization

Septembe

CYBER HYGIENE REPORT CARD

For Official Use Only (FOUO)

HIGH LEVEL FINDINGS

ADDRESSES 48 ↔ no change

HOSTS 18 ↑ 8 increase

SERVICES 18 ↑ 4 increase

VULNERABILITIES 16 ↓ 8 decrease

VULNERABILITIES

CRITICAL 0 ↔ 0 resolved 0 new

HIGH 2 ↔ 0 resolved 0 new

MEDIUM 2 ↓ 8 resolved 0 new

LOW 12 ↔ 2 resolved 2 new

PREVIOUS REPORT ● resolved

CURRENT REPORT ● new

ORGANIZATIONAL COMPARISONS

VULNERABLE HOST SCORE 4.0 ↓ 1.6 better

OVERALL SCORE 2.2 ↓ 2.8 better

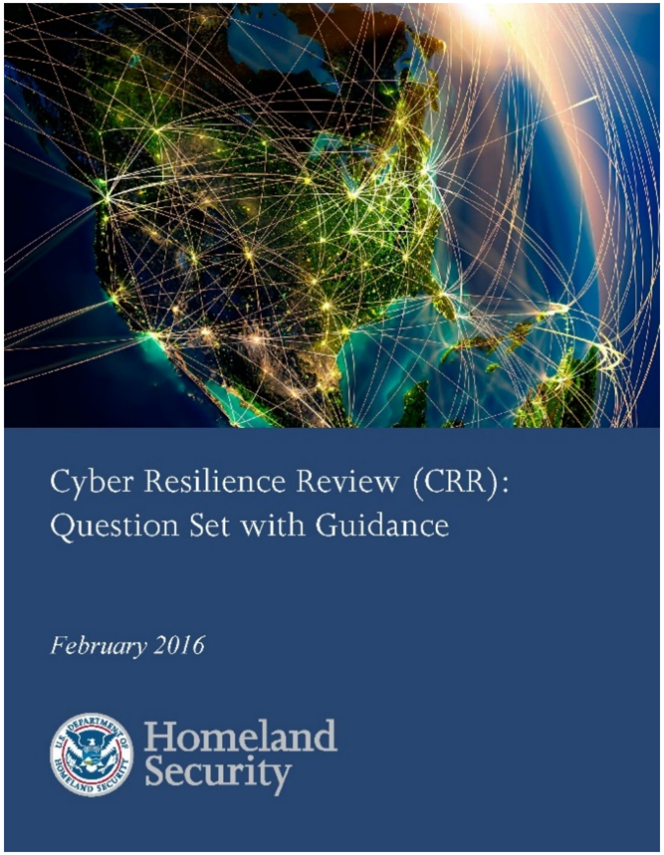
CYBER RESILIENCE REVIEW

Cyber Resilience Review

- **Purpose:** Evaluate operational resilience and cybersecurity practices of **critical services.**

- Delivery: Either
  - CSA-facilitated, or
  - Self-administered

- Benefits include: Helps public and private sector partners understand and measure cybersecurity capabilities as they relate to operational resilience and cyber risk



Cyber Resilience Review (CRR):
Question Set with Guidance

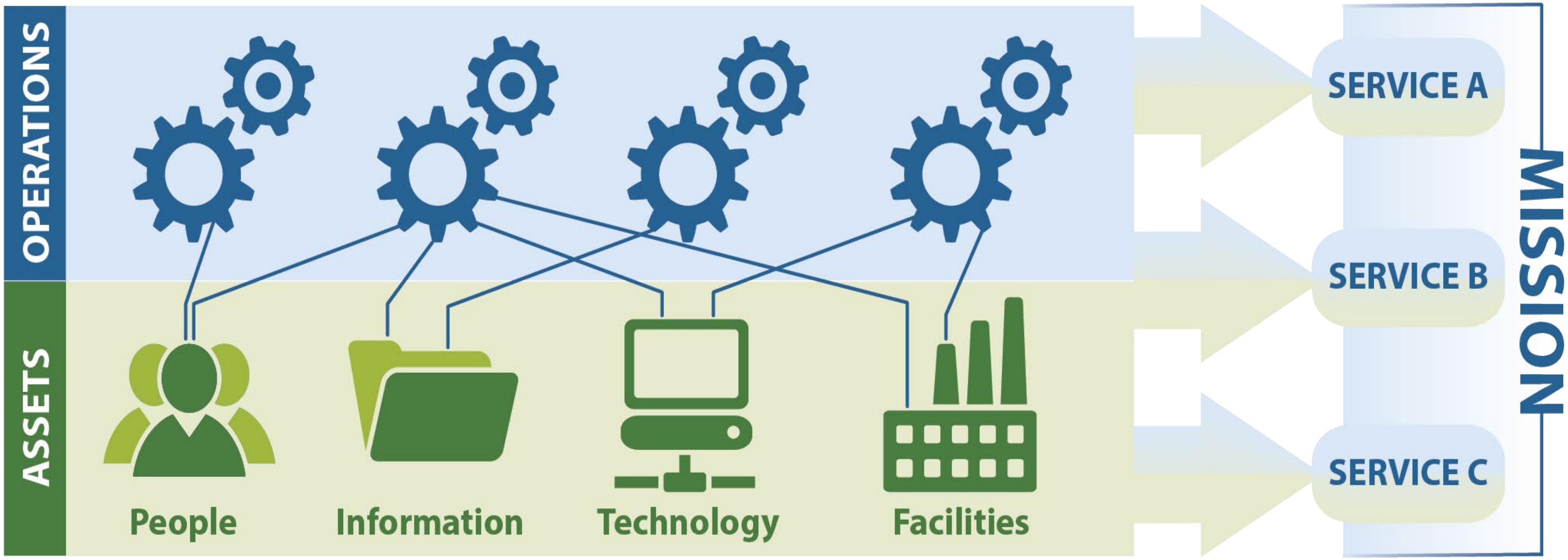
February 2016

Homeland
Security

CRR Question Set & Guidance

Critical Service Focus

Organizations use **assets (people, information, technology, and facilities)** to provide operational **services** and accomplish **missions**.



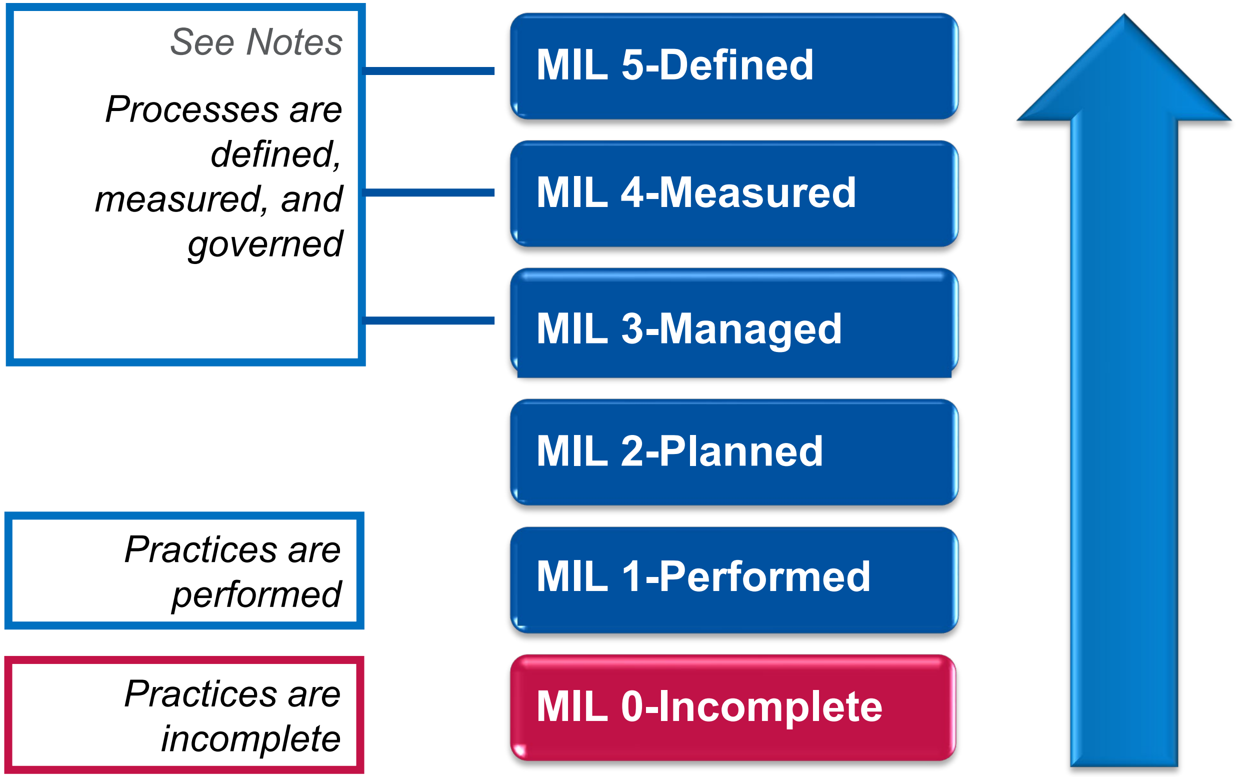
Cyber Resilience Review Domains

Asset Management Know your assets being protected & their requirements, e.g., CIA	**Risk Management** Know and address your biggest risks that considers cost and your risk tolerances
Configuration and Change Management Manage asset configurations and changes	**Service Continuity Management** Ensure workable plans are in place to manage disruptions
Controls Management Manage and monitor controls to ensure they are meeting your objectives	**Situational Awareness** Discover and analyze information related to immediate operational stability and security
External Dependencies Management Know your most important external entities and manage the risks posed to essential services	**Training and Awareness** Ensure your people are trained on and aware of cybersecurity risks and practices
Incident Management Be able to detect and respond to incidents	**Vulnerability Management** Know your vulnerabilities and manage those that pose the most risk

For more information: http://www.us-cert.gov/ccubedvp

Process Institutionalization

CRR maturity indicator levels (MILs) are to measure process institutionalization:



See Notes

Processes are defined, measured, and governed

Practices are performed

Practices are incomplete

MIL 5-Defined

MIL 4-Measured

MIL 3-Managed

MIL 2-Planned

MIL 1-Performed

MIL 0-Incomplete

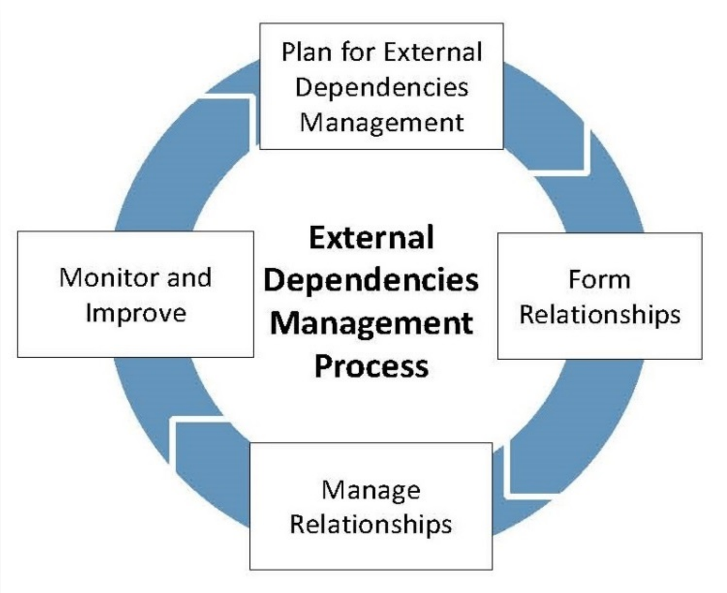
Higher MIL degrees translate to more stable processes that:

- Produce consistent results over time
- Are retained during times of stress

EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENT

External Dependencies Management Assessment

- **Purpose:** Evaluate an entity’s management of their dependencies on third-party entities
- **Delivery:** CSA-facilitated
- **Benefits**:
  - Better understanding of the entity’s cyber posture relating to external dependencies
  - Identification of improvement areas for managing third parties that support the organization


Plan for External Dependencies Management
External Dependencies Management Process
Form Relationships
Manage Relationships
Monitor and Improve

EDM process outlined per the External Dependencies Management Resource Guide

EDM Assessment Organization and Structure

- Structure and scoring similar to Cyber Resilience Review
- Uses one Maturity Indicator Level (MIL) scale with three lifecycle domains.

Relationship Formation

Assesses whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them.

Relationship Management and Governance

Assesses whether the acquirer manages ongoing relationships to maintain the resilience of the critical service, and mitigate dependency risk.

Service Protection and Sustainment

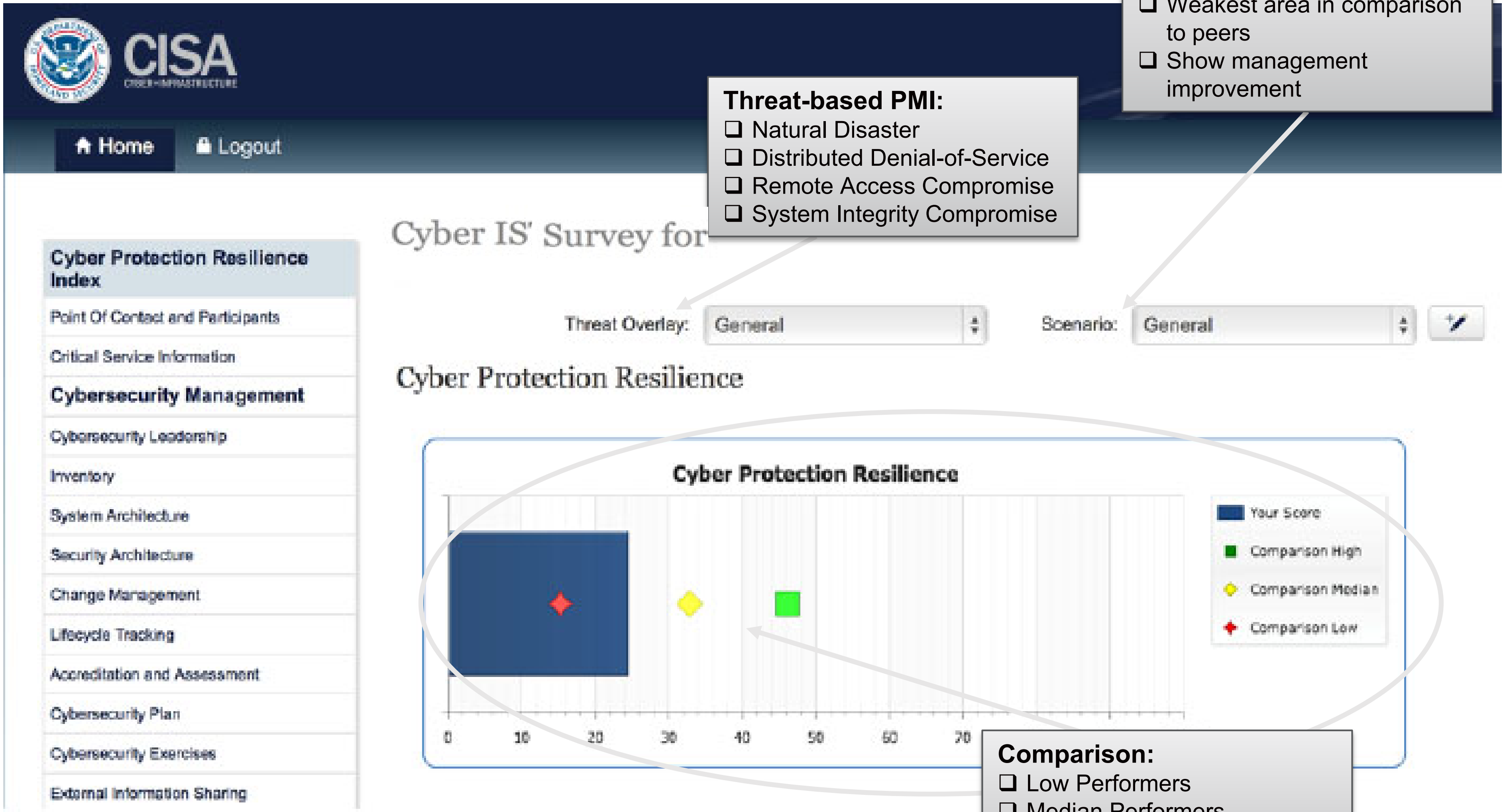
Assesses whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents, disruptions, and threats.

CYBER INFRASTRUCTURE SURVEY

Cyber Infrastructure Survey Highlights

- Purpose: Evaluate security controls, cyber preparedness, overall resilience.
- Delivery: CSA-facilitated
- Benefits:
  - Effective assessment of cybersecurity controls in place for a critical service,
  - Easy-to-use interactive dashboard to support cybersecurity planning and resource allocation), and
  - Access to peer performance data visually depicted on the dashboard.

Example of CIS Dashboard



CISA CYBER+INFRASTRUCTURE

🏠 Home 🔒 Logout

Cyber Protection Resilience Index

Point Of Contact and Participants

Critical Service Information

Cybersecurity Management

Cybersecurity Leadership

Inventory

System Architecture

Security Architecture

Change Management

Lifecycle Tracking

Accreditation and Assessment

Cybersecurity Plan

Cybersecurity Exercises

External Information Sharing

Cyber IS' Survey for

Threat Overlay: General

Scenario: General

Cyber Protection Resilience

Threat-based PMI:

- ❑ Natural Disaster
- ❑ Distributed Denial-of-Service
- ❑ Remote Access Compromise
- ❑ System Integrity Compromise

Scenario:

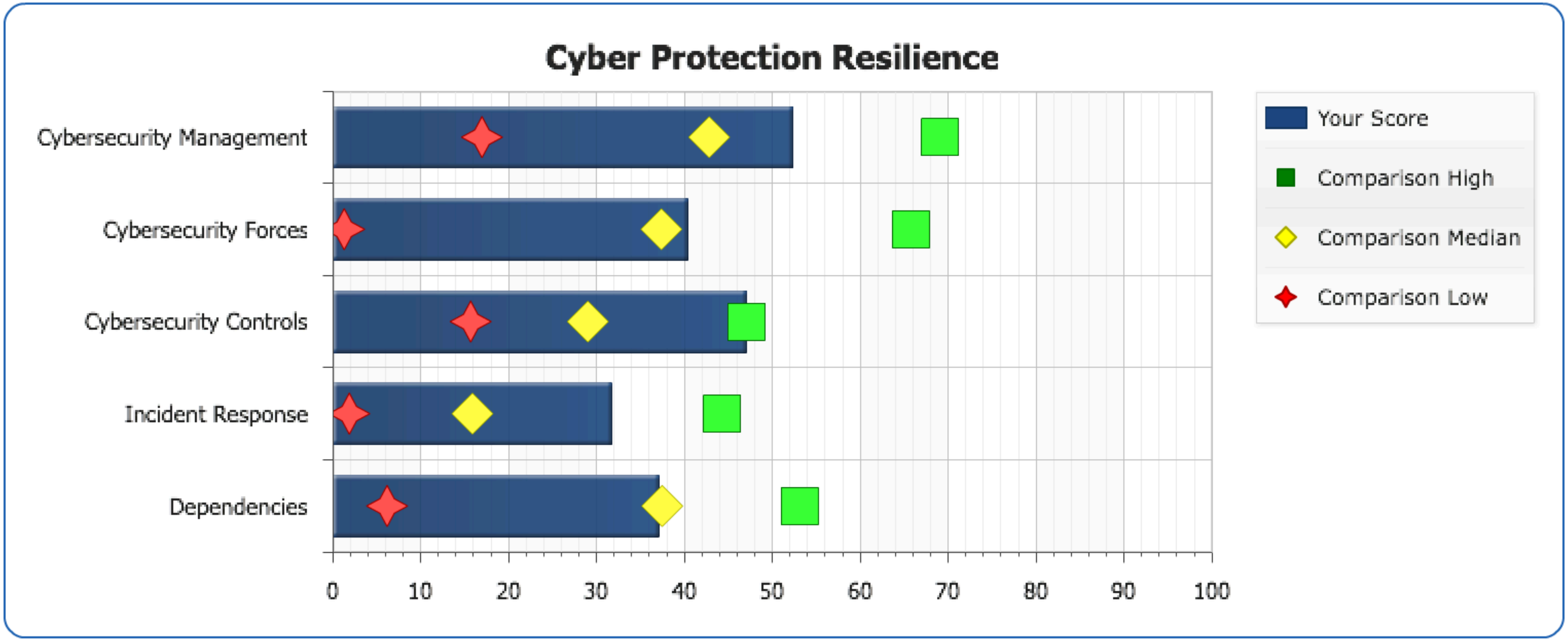
- ❑ Where should we to invest?
- ❑ Weakest area in comparison to peers
- ❑ Show management improvement

Comparison:

- ❑ Low Performers
- ❑ Median Performers
- ❑ High Performers

CIS Dashboard - Comparison

- Shows the low, median, and high performers
- Compares your organization to the aggregate



CYBER SECURITY EVALUATION TOOL

Cyber Security Evaluation Tool

- **Purpose:** Assesses control system and information technology network security practices against industry standards.
- **Facilitated:** Self-Administered, undertaken independently
- **Benefits:**
  - Immediately available for download upon request
  - Understanding of operational technology and information technology network security practices
  - Ability to drill down on specific areas and issues
  - Helps to integrate cybersecurity into current corporate risk management strategy

PHISHING CAMPAIGN ASSESSMENT

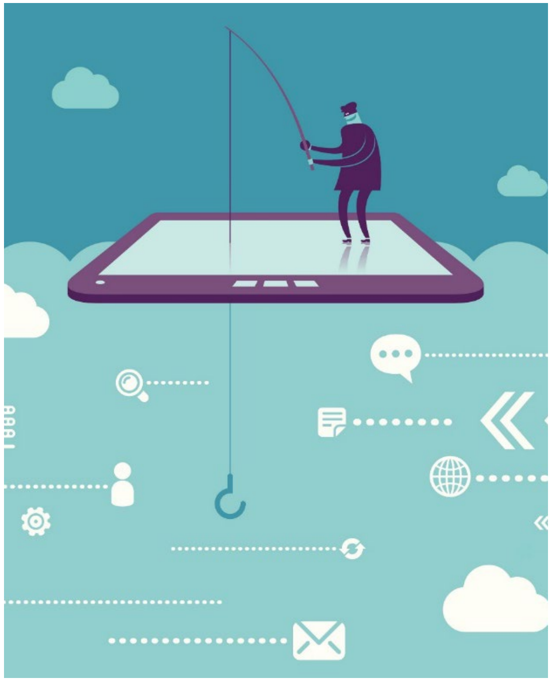
Phishing Campaign Assessment

Purpose: Test an organization’s susceptibility and reaction to phishing emails.

Delivery: Online delivery by CISA

Benefits:

- Identify the risk phishing poses to your organization
- Decrease risk of successful malicious phishing attacks, limit exposure, reduce rates of exploitation
- Receive actionable metrics
- Highlight need for improved security training
- Increase cyber awareness among staff



Phishing Campaign Assessment Sample Email, 1 of 2

To: <Stakeholder List>

From: Apples Customer Relations <freeapplesforyou@[PCA-testing-site].org> Subject: Free iPad – Just Complete a Survey!

Want the new iPad or iPad Mini? I got mine free from this site: <fake link> !!!!!

We would like to invite you to be part of a brand new pilot program to get our new product in the hands of users before official release. This assures that any issues or errors are mitigated before the release. If you are accept to participate in this programall we ask is that you submit a survey at the end of the Pilot. You be able to keep iPad at the end for free!

Apples Customer Relationships Office

Apples Campus, Cupertino, California 95114

Phishing Campaign Assessment Sample Email, 2 of 2

To: <Stakeholder List>
From: OBRM <OBRM@[PCA-testing-site].org>
Subject: Future Budget Plans

In the coming weeks, our state’s leadership will be working to draft a plan to prevent long term financial issues and ways to avoid human resource reductions. All departments within the State Government are being directed to draft a plan to help meet projected budget shortages and find ways to reduce spending within the State Government.

We have been asked to work more efficiently with less. As a result, many budgets and programs are also facing significant reduction. The Office of Budget and Resource Management has developed a draft plan that will address any potential budget shortcomings.

To learn more about the budget and how your program maybe affected, please visit <LINK>.

If you have any questions or concerns, we’d love to hear them. Please emails us here <embedded link>.

Office of Budget and Resource Management

VALIDATED ARCHITECTURE DESIGN REVIEW

Validated Architecture Design Review

Purpose: Analyze network architecture, system configurations, log file review, network traffic and data flows to identify abnormalities in devices and communications traffic.

Delivery: CISA staff working with entity staff

Benefits:

- In-depth review of network and operating system
- Recommendations to improve an organization’s operational maturity and enhancing their cybersecurity posture
- Evaluation of network architecture

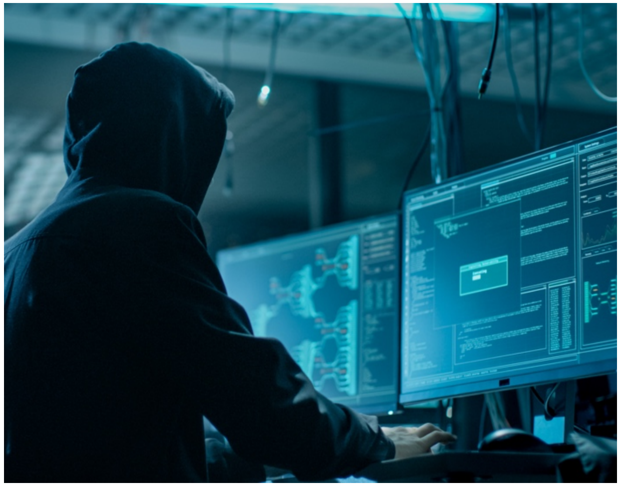
CISA
CYBER+INFRASTRUCTURE

RISK AND VULNERABILITY ASSESSMENT

[PENETRATION TEST]

Risk and Vulnerability Assessment

- **Purpose**: Perform network penetration and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks
- **Delivery**: Onsite by CISA
- **Benefits**:
  - Identification of vulnerabilities
  - Specific remediation recommendations
  - Improves an entity's cyber posture, limits exposure, reduces rates of exploitation
  - Increases speed and effectiveness of future cyber attack responses.



CISA
CYBER+INFRASTRUCTURE

Risk and Vulnerability Assessment Specifics

Assessment Aspects

Service	Description
Vulnerability Scanning and Testing	Conduct Vulnerability Assessments
Penetration Testing	Exploit weakness, test responses in systems, applications, network, and security controls
Social Engineering	Craft e-mail at targeted audience to test security awareness, used as an attack sector to internal network
Wireless Discovery & Identification	Identify wireless signals and rogue wireless devices, and exploit access points
Web Application Scanning and Testing	Identify web application vulnerabilities
Database Scanning	Security Scan of database settings and controls
Operating System Scanning	Security Scan of operating system to do compliance checks

Incident Reporting

NCCIC (ICS-CERT/US-CERT) INCIDENT REPORTING INFORMATION

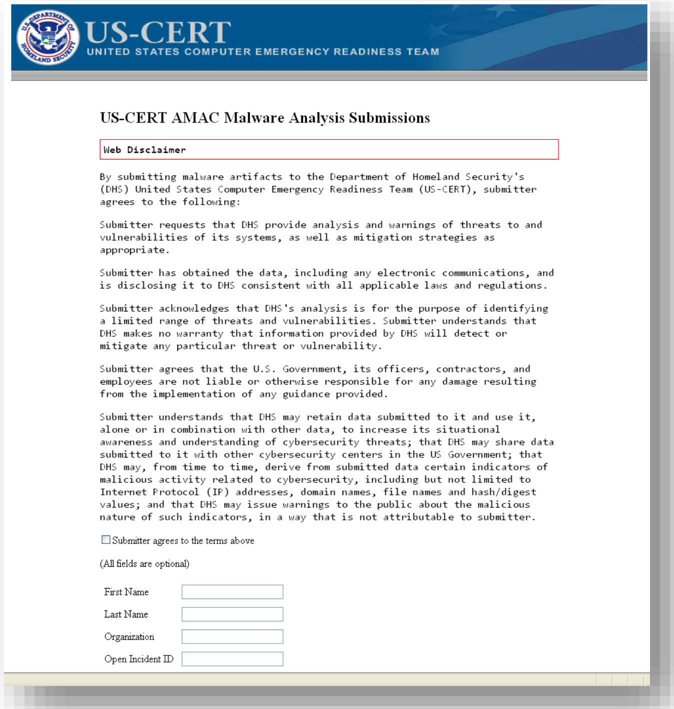
Additional - Incident Reporting

NCCIC provides real-time threat analysis and incident reporting capabilities

- 24x7 contact number: 1-888-282-0870

Malware Submission Process:

- Please send all submissions to AMAC at: submit@malware.us-cert.gov
- Must be provided in password-protected zip files using password “infected”
- Web-submission: https://malware.us-cert.gov



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

US-CERT AMAC Malware Analysis Submissions

Web Disclaimer

By submitting malware artifacts to the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT), submitter agrees to the following:

Submitter requests that DHS provide analysis and warnings of threats to and vulnerabilities of its systems, as well as mitigation strategies as appropriate.

Submitter has obtained the data, including any electronic communications, and is disclosing it to DHS consistent with all applicable laws and regulations.

Submitter acknowledges that DHS's analysis is for the purpose of identifying a limited range of threats and vulnerabilities. Submitter understands that DHS makes no warranty that information provided by DHS will detect or mitigate any particular threat or vulnerability.

Submitter agrees that the U.S. Government, its officers, contractors, and employees are not liable or otherwise responsible for any damage resulting from the implementation of any guidance provided.

Submitter understands that DHS may retain data submitted to it and use it, alone or in combination with other data, to increase its situational awareness and understanding of cybersecurity threats; that DHS may share data submitted to it with other cybersecurity centers in the US Government; that DHS may, from time to time, derive from submitted data certain indicators of malicious activity related to cybersecurity, including but not limited to Internet Protocol (IP) addresses, domain names, file names and hash/digest values; and that DHS may issue warnings to the public about the malicious nature of such indicators, in a way that is not attributable to submitter.

☐ Submitter agrees to the terms above

(All fields are optional)

First Name ______

Last Name ______

Organization ______

Open Incident ID ______

Any Questions/Discussion?

- Web Resources and Contact CheatSheet:
- ICS-Cert: https://ics-cert.us-cert.gov/
- Stakeholder Engagement and Cyber Infrastructure Resilience:

  http://www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience

Contact Information

Evaluation Inquiries

cyberadvisor@hq.dhs.gov

General Inquiries

Region4CSA@cisa.dhs.gov

Klint Walker Cyber Security Advisor, Region IV	Klint.walker@hq.dhs.gov +1 404-895.1127
Jason Burt Cyber Security Advisor, Region IV	Jason.Burt@cisa.dhs.gov +1 202-578-9954

Department of Homeland Security
National Protection and Programs Directorate
Office of Cybersecurity and Communications

CYBER SECURITY SELF-TEST - 1

What role do you play in IT security, IT incident response, IT continuity of operations?

- Planner, Responder, Investigator?

How much emphasis do you place upon having up-to-date, documented plans versus having available, capable staff?

- What types of cyber hazards do these plans account for?

What requirements have you provided to IT security personnel and IT continuity planners, in terms of goals and objectives your agency/organization wants to achieve for cyber security?

- Do you have a procedures in-place that triggers your participation and coordination in incident response, continuity operations, etc?

How do you and do you test IT incident response and continuity plans beforehand?

- What makes a good test?
- How much are your disruptive scenarios based upon real-world threats?

CYBER SECURITY SELF-TEST - 2

How would law enforcement coordinate with you as an affected organizations, in the wake of cyber attacks?

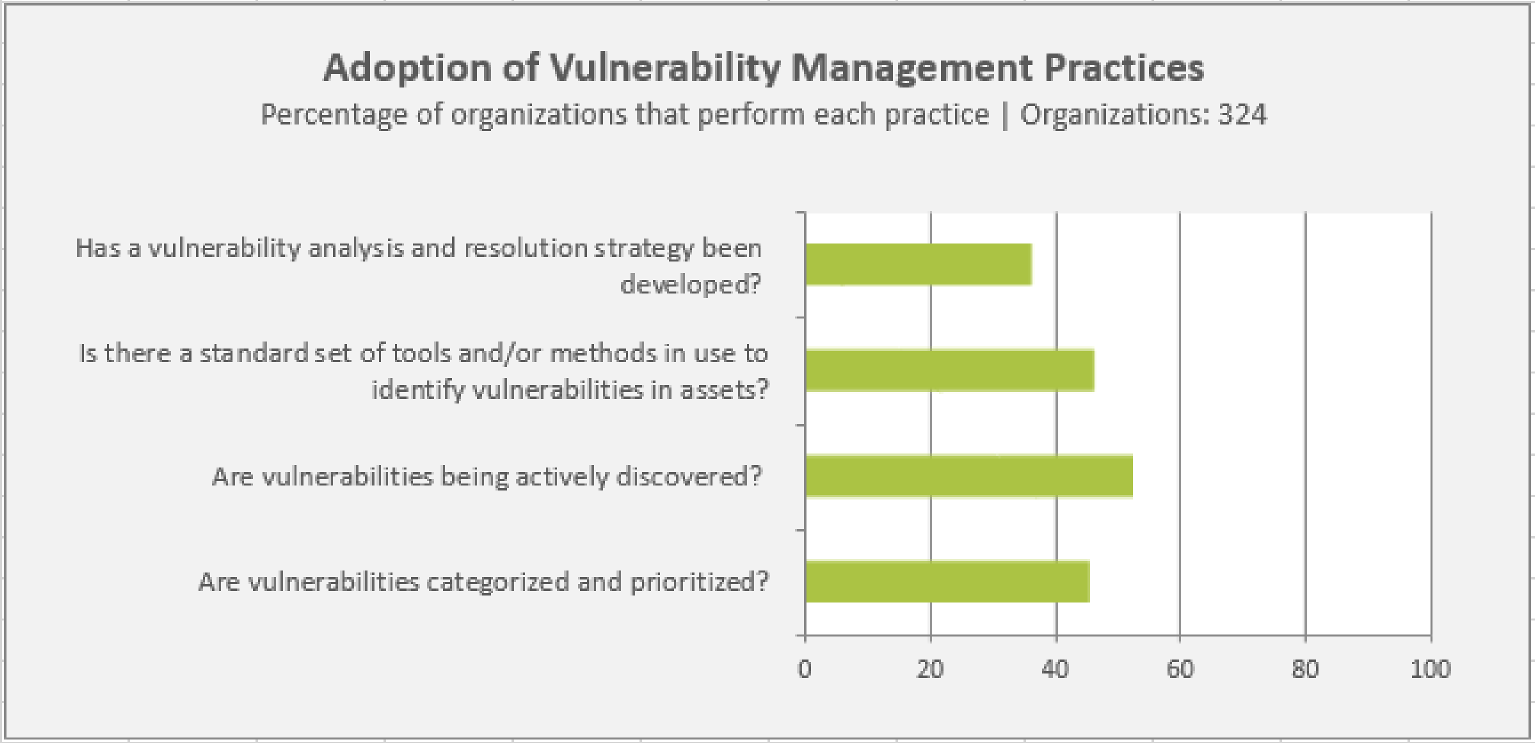
Who in your agency or organization is (best) authorized to contact outsider partners (e.g., contracted, private, public, etc) for help, assistance, response, etc?

What do you want to know in the first 30 minutes of a disruptive cyber attack?

What are you willing to share within the first 30 minutes of a disruptive cyber attack?

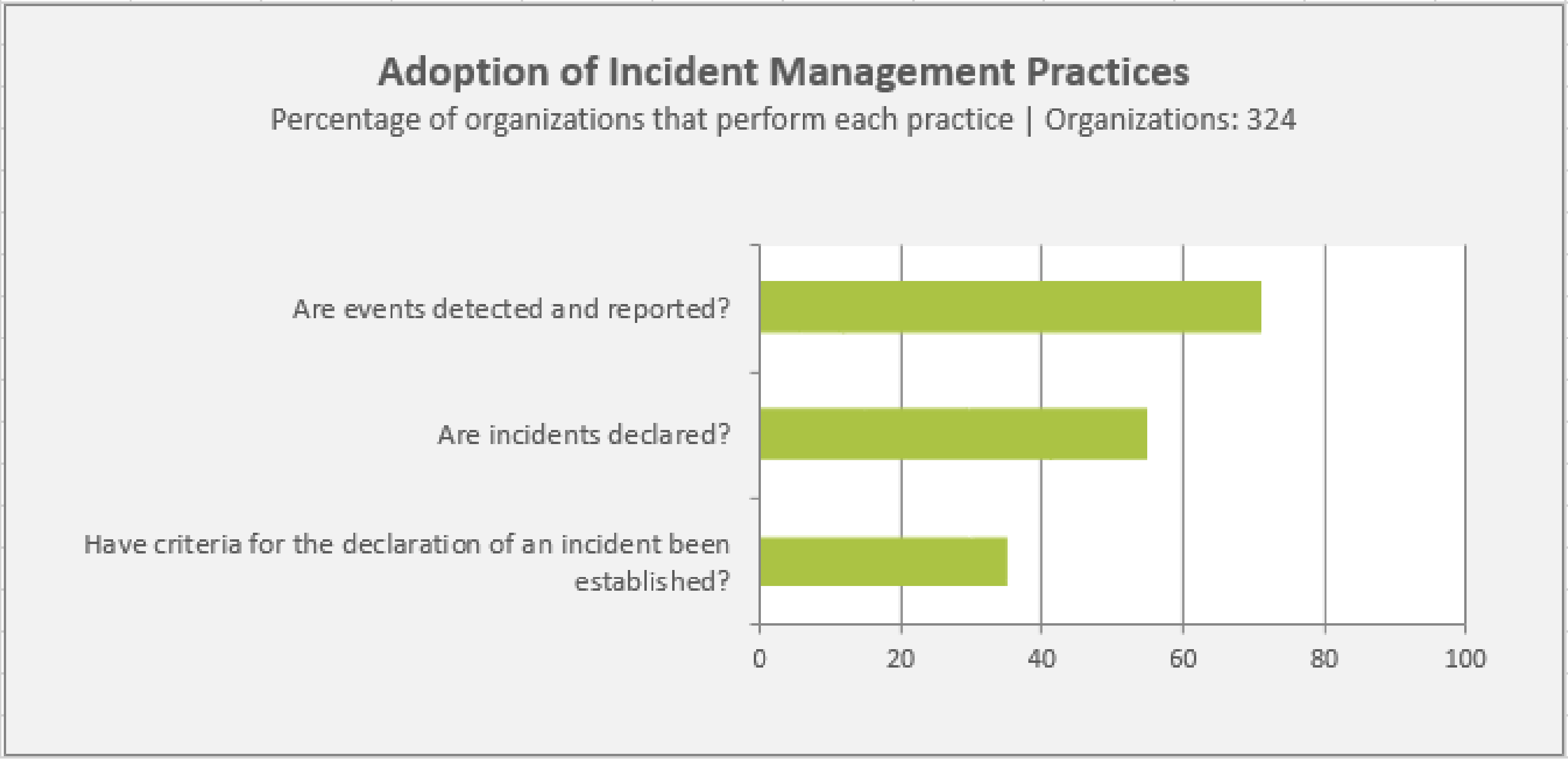
What steps are you going to take in the next 30 days to improve cyber security … at the office … in your operations … at home?

Vulnerability Management



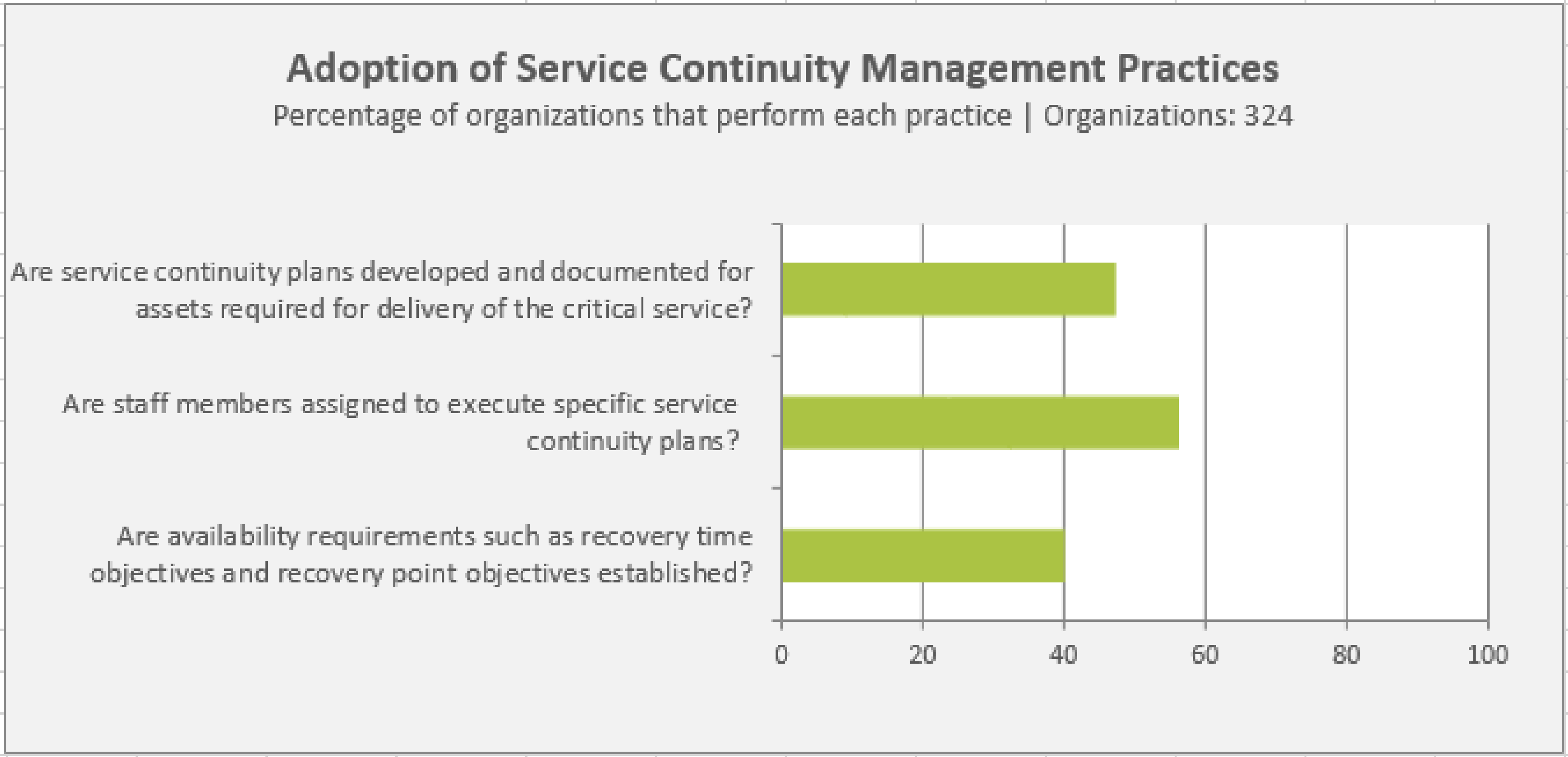
- Approximately 35% of organizations have a strategy to guide their vulnerability management efforts.
- Roughly 45% of organizations have determined a standard set of tools or methods to assist in identifying vulnerabilities.

Incident Management



- While roughly 70% of organizations perform event detection
    - 55% have a process to declare incidents
    - and only 35% have developed criteria to guide their staff

Service Continuity



- Less than 50% of organizations have documented service continuity plans.
- Only 40% specify recovery time and recovery point objectives in their plans.