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

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.

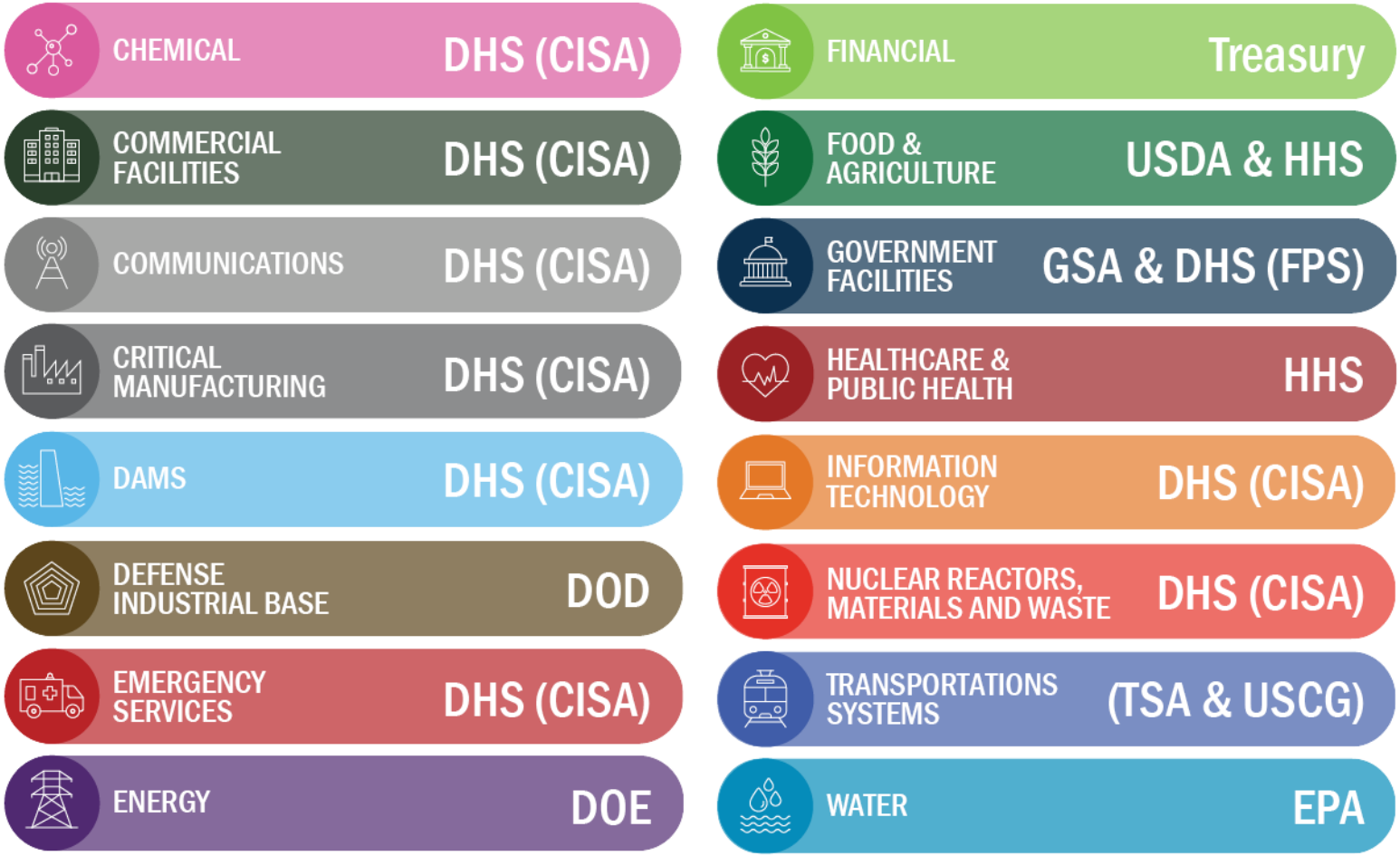
FEDERAL NETWORK PROTECTION

PROACTIVE CYBER PROTECTION

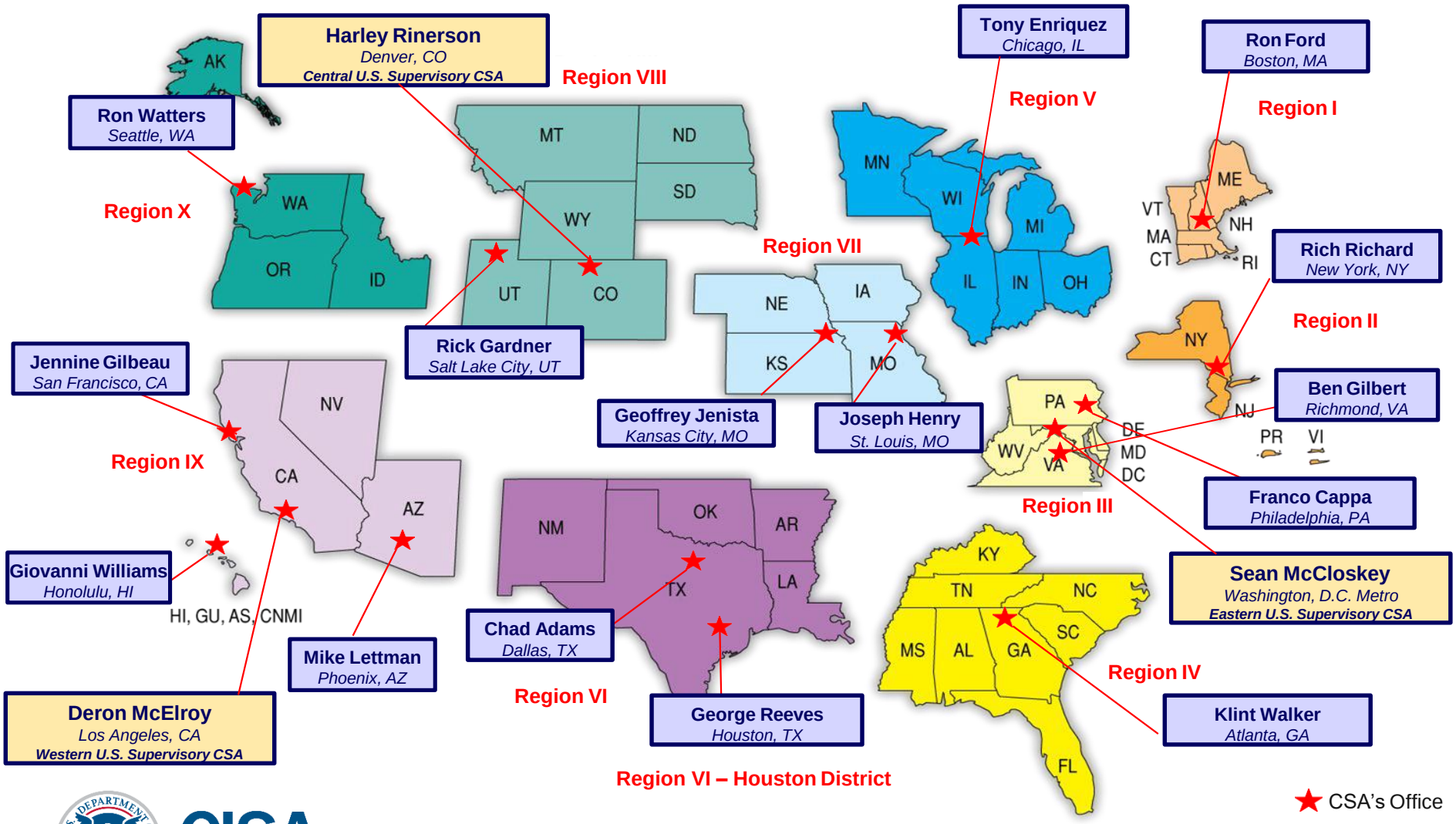
INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS

EMERGENCY COMMUNICATIONS

16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies



CSA Deployed Personnel



CISA
CYBER+INFRASTRUCTURE

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

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

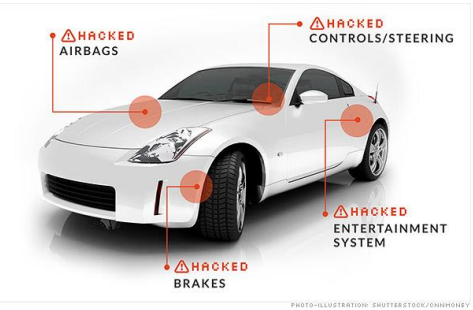
Homeland Security

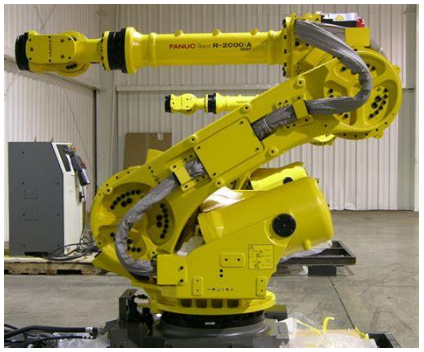
Cyber Security is Critical

- 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

Our transport





Our Production

Our health

Homeland Security

Many things to go wrong

200M lines of code in a modern vehicle!

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

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

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

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

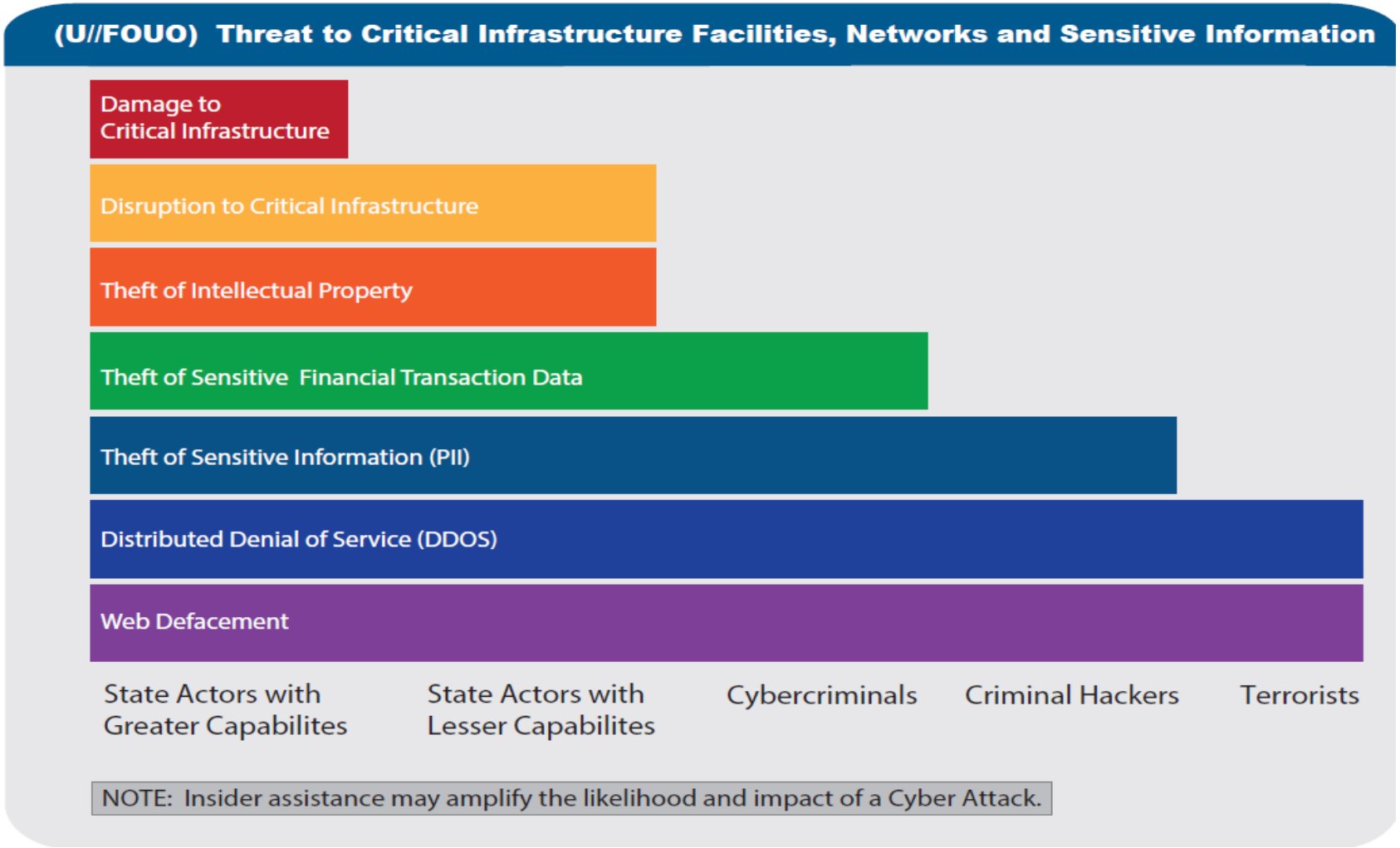
Homeland Security
Science and Technology

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.

Homeland Security

Threat Landscape



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**

SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
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

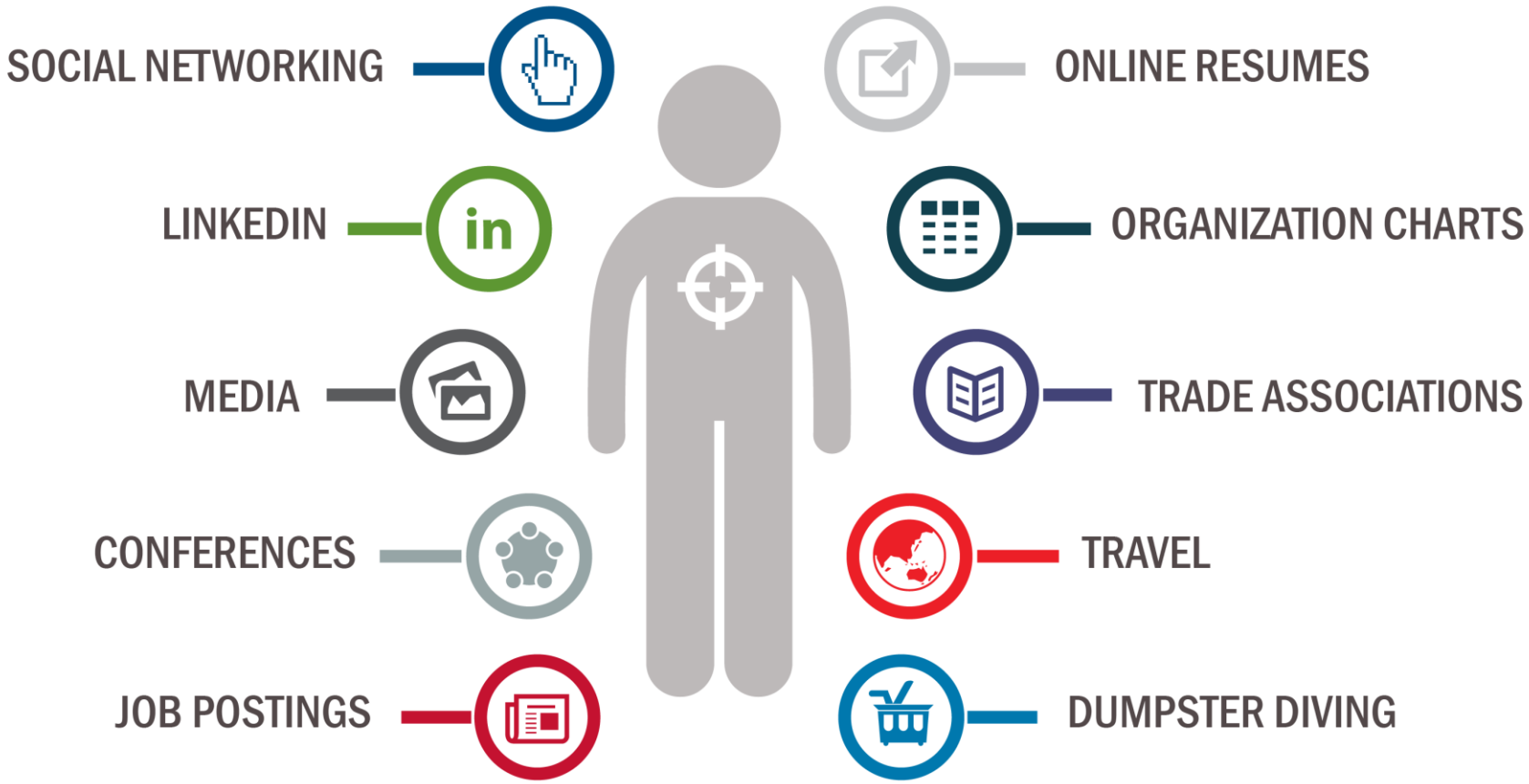
In a recent poll over 50 percent of organizations have had a breach that was caused by one of their vendors

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

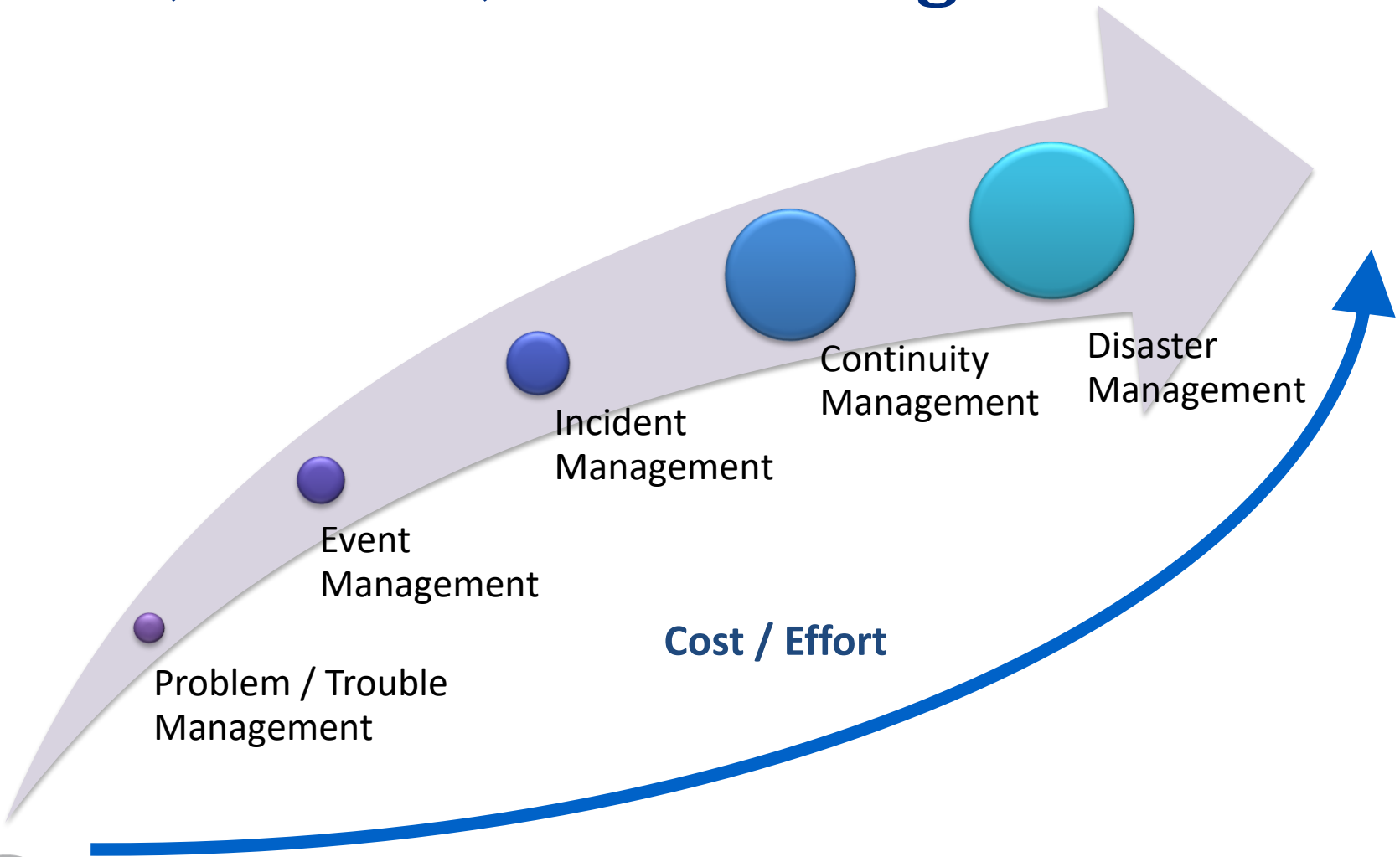
Cyber Supply Chain Threats

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 Threat Actors?



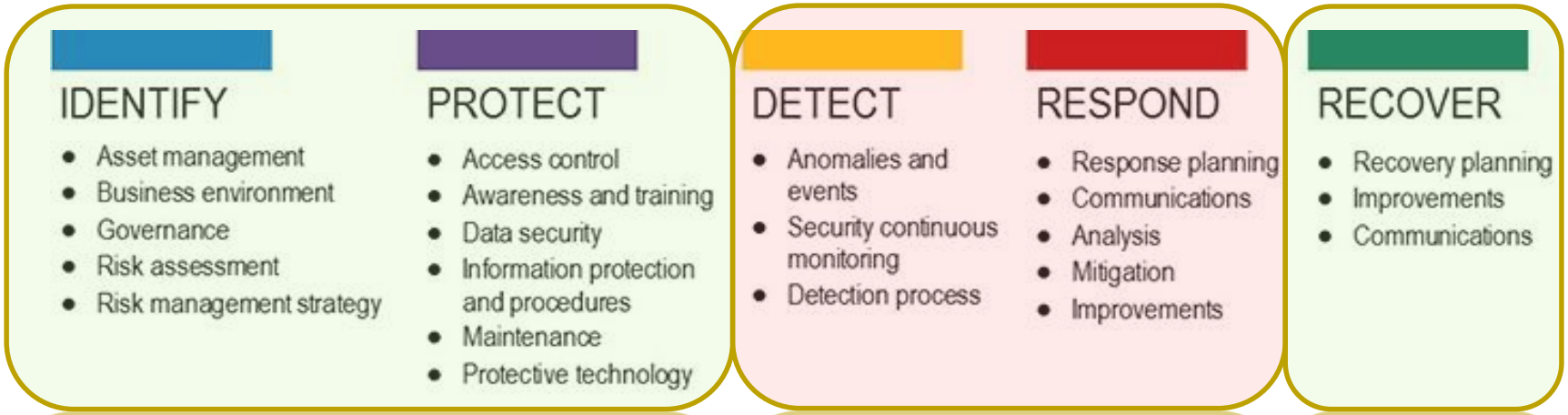
Operational Planning for Cyber Security Events, Attacks, and Contingencies



Homeland Security

CSF and the State of Cybersecurity Management

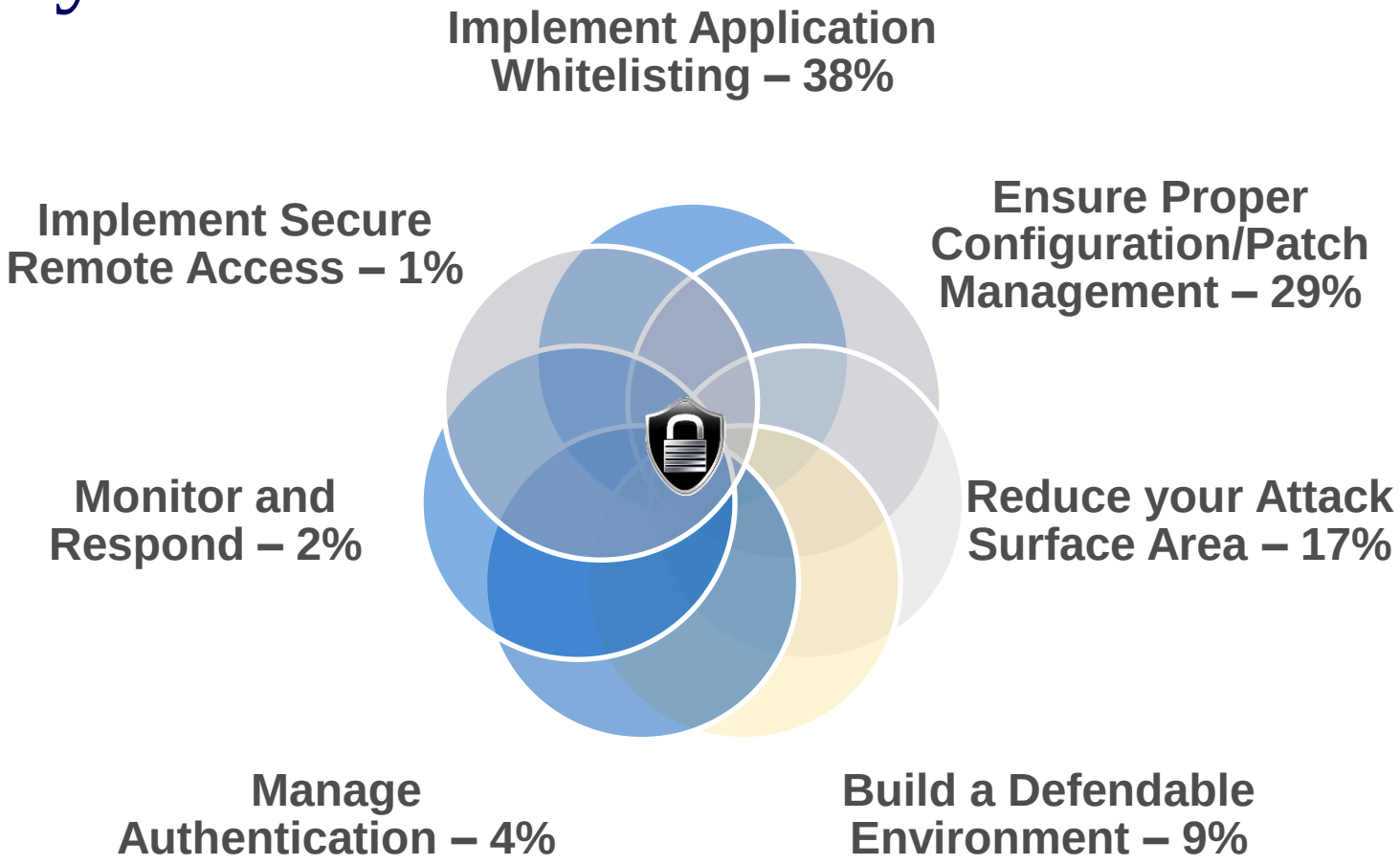
Status Quo: Practiced, Planned, & Resourced



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

Homeland Security

Incident Response Root Cause Analysis



Homeland Security

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?

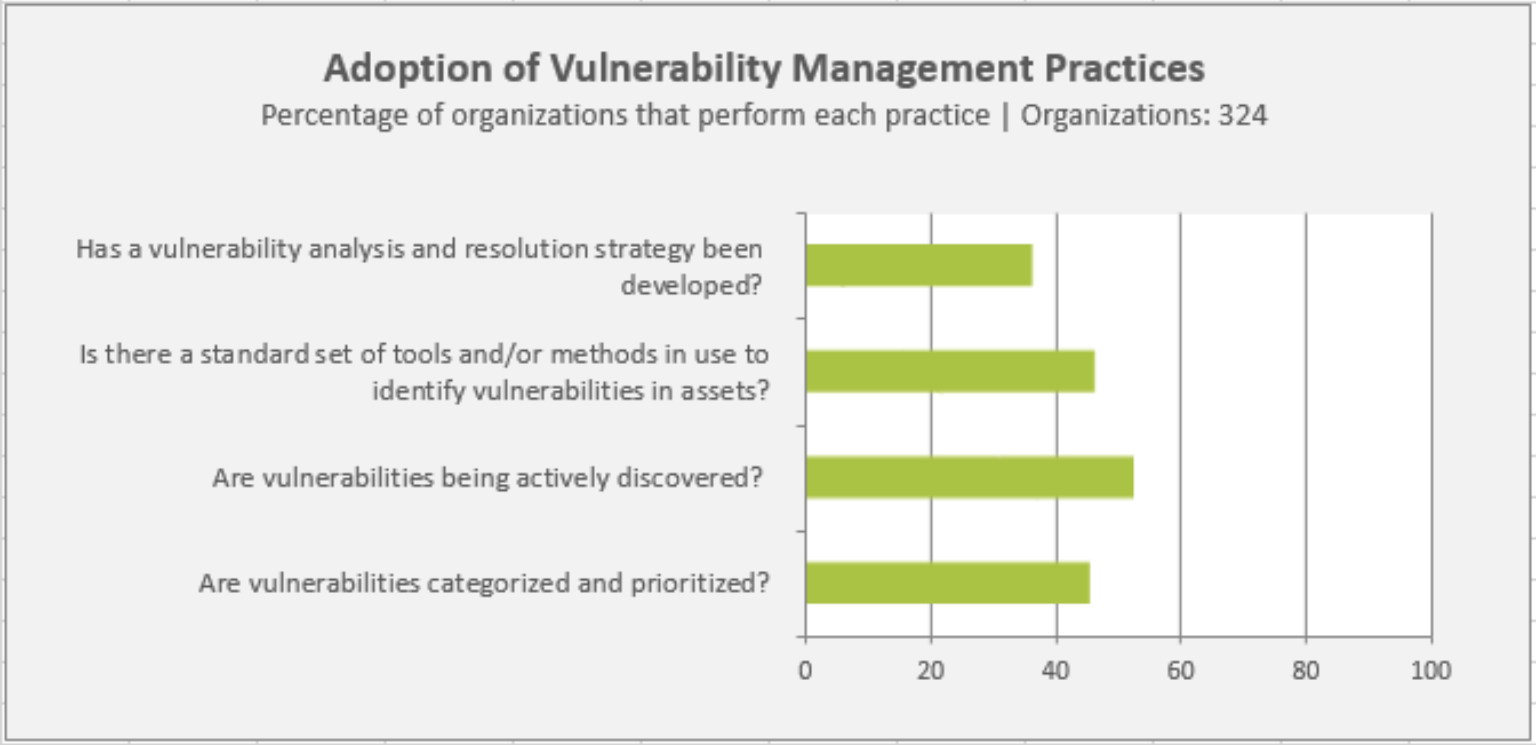
What do you want to know in the first 30 minutes of a disruptive cyber attack?

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?

Homeland Security

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.

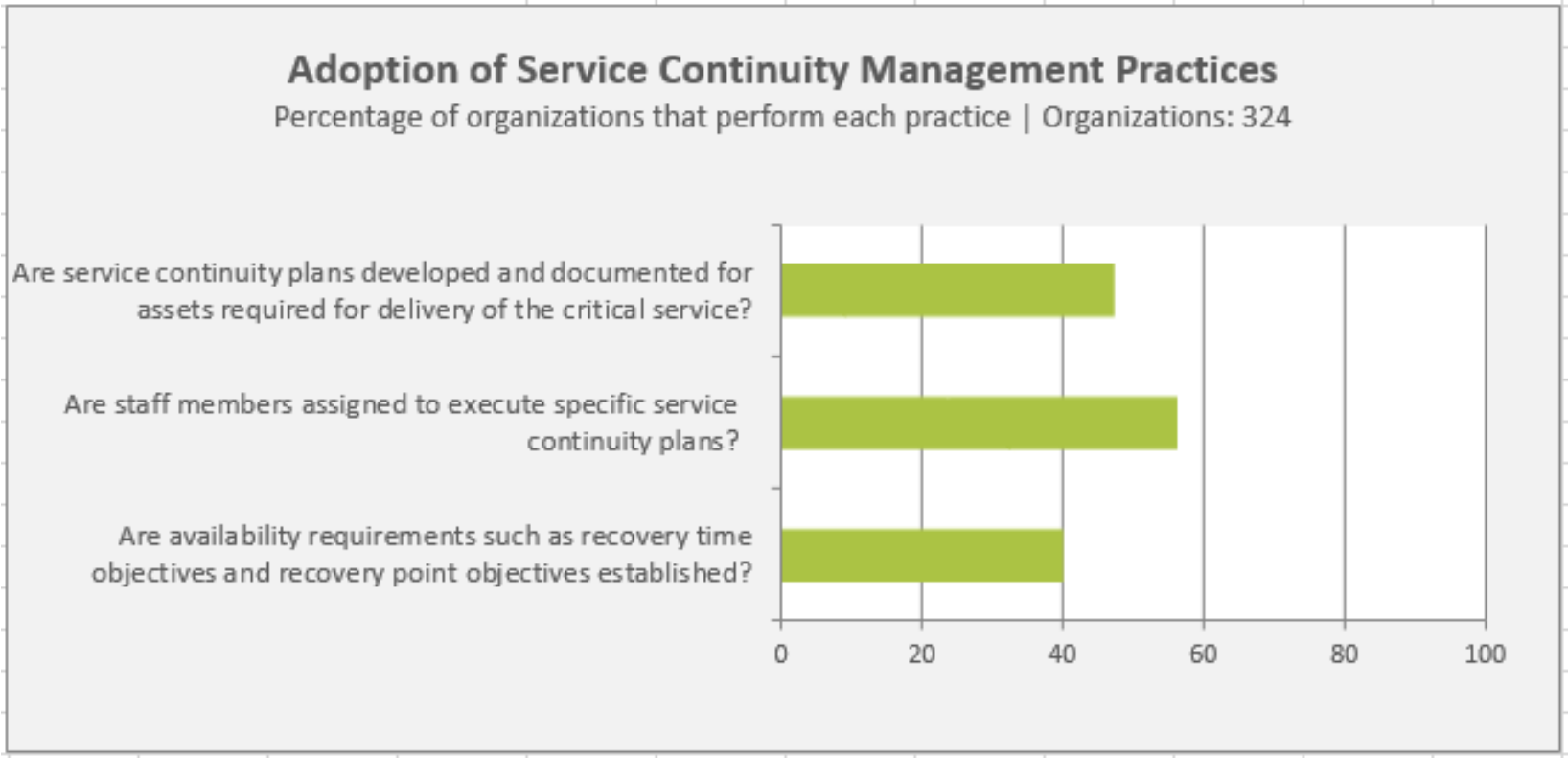
Homeland Security

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

Homeland Security

Service Continuity



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

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

CISA
CYBER+INFRASTRUCTURE

Range of Cybersecurity Assessments

- 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)----------

STRATEGIC
(C-Suite Level)

TECHNICAL
(Network-Administrator Level)

CISA
CYBER+INFRASTRUCTURE

Incident Reporting

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

Homeland Security

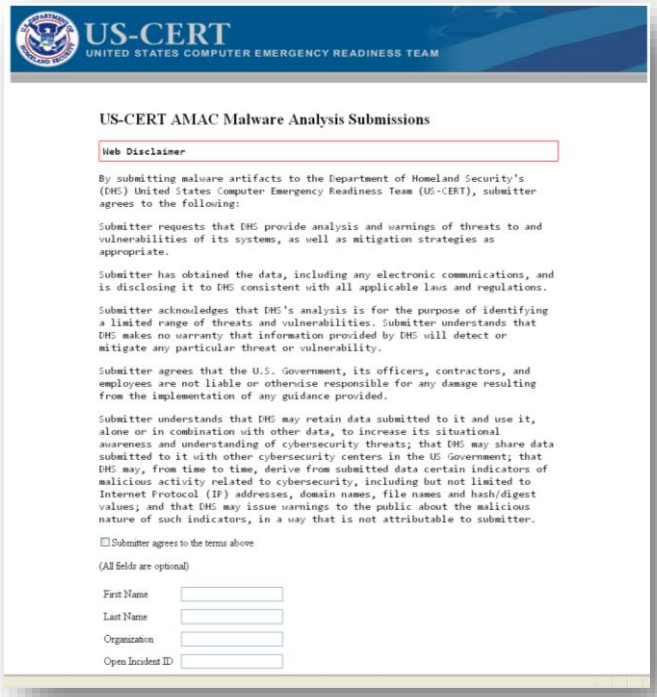
Additional - Incident Reporting

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

Homeland Security

Contact Information

Evaluation Inquiries
cyberadvisor@hq.dhs.gov

General Inquiries
cyberadvisor@hq.dhs.gov

DHS Contact Information	
Klint Walker Cyber Security Advisor, Region IV	Klint.walker@hq.dhs.gov +1 404-895.1127

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