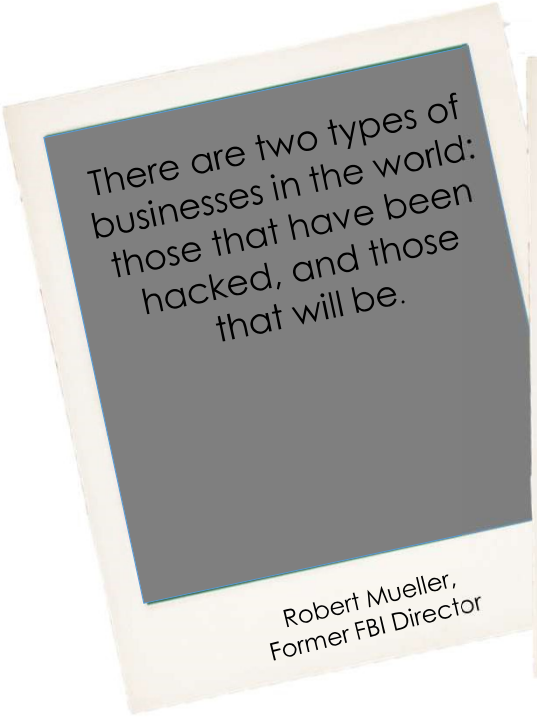
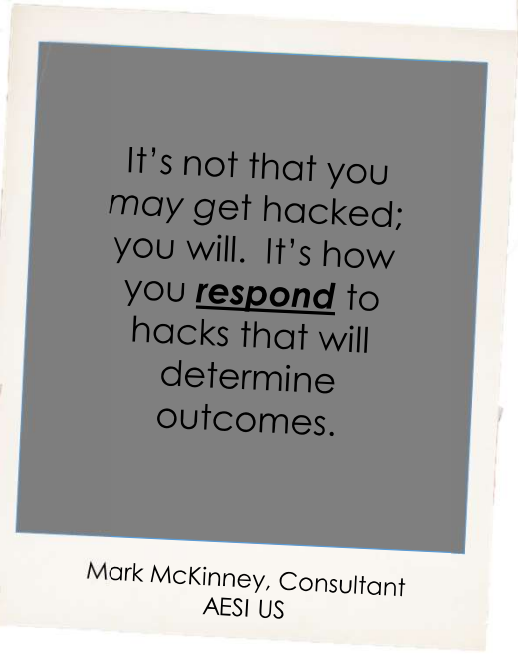
Southeast Regional Municipal Utility Cybersecurity Summit 2019

Plan For and Execute Successful Incident Response Policies and Procedures

Mark McKinney CISSP, CISA, CFE, CCFE
Director, Cyber Security
AESI – US, Inc.
markm@aesi-inc.com
770.870.1630 x. 279 · US

The Not-so-New Reality



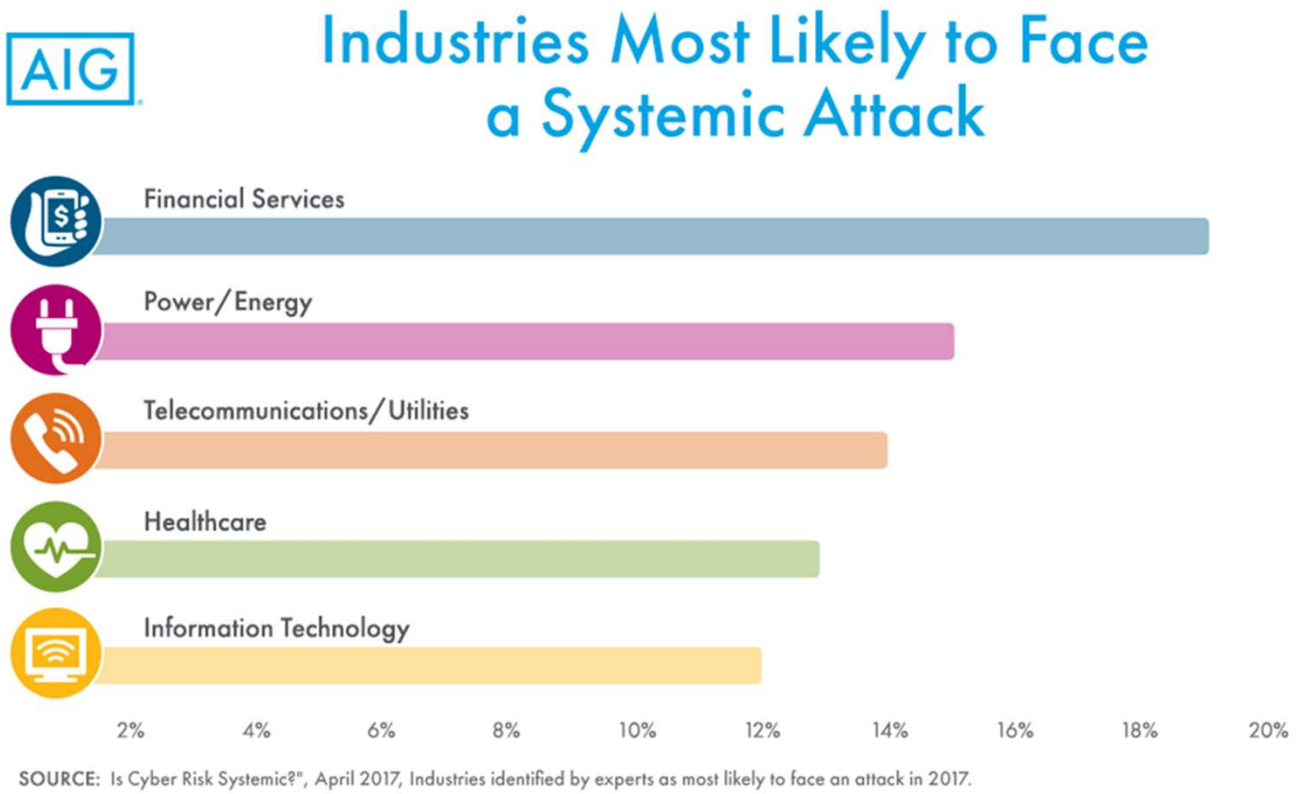


Cyber Crime

$6T	Estimated global cost of cyber crime expected to exceed $6T by 2021. Up from $3T in 2015, and $600B in 2014.
+30K	FBI Internet Crimes Complaint Center vetted 301,580 complaints in 2017, up from 269,422 in 2014. *4,063,933 since 2000*.
3000+	Estimated number of cyber attempts against U.S. energy sector annually.

Common incidents involve impersonation e-mail scams, various intimidation crimes, and scams that used computer “scareware” to extort money or proprietary information from various user types, also referred to as phishing scams.

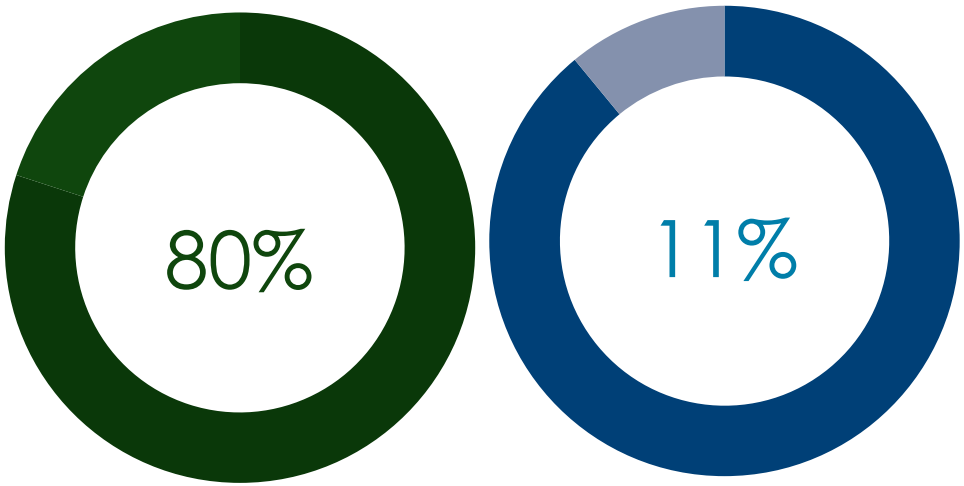
Targeted Industries



SOURCE: Is Cyber Risk Systemic?", April 2017, Industries identified by experts as most likely to face an attack in 2017.

Energy Utilities

According to a recent Trustwave study, the energy sector now accounts for up to 80 percent of reported cyber incidents and data breach investigations, with e-commerce attacks emerging as the growing trend, followed by control center operations and distributed grid infiltrations.



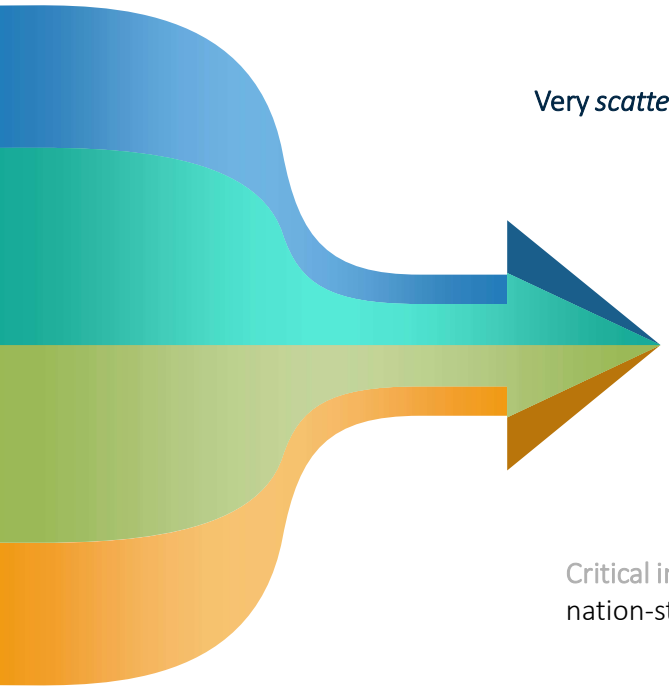
A 2016 DoE Idaho National Laboratory Mission Support Center report notes that 80 percent of power and utility companies reported an increase in threats with mobile computing, malware, and phishing being of greatest concern. However, ***"only 11% of survey respondents said they felt their current information security measures fully meet their organization's needs, 60% are running no or informal threat assessments while 64% believe that their security strategy is not aligned with today's risk environment."***

Trustwave 2018 Global Security Report

Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector; U.S. Department of Energy, Idaho National Laboratory, Mission Support Center

Energy Utilities are Lucrative Targets

Estimated over 2 million interconnected SCADA systems worldwide

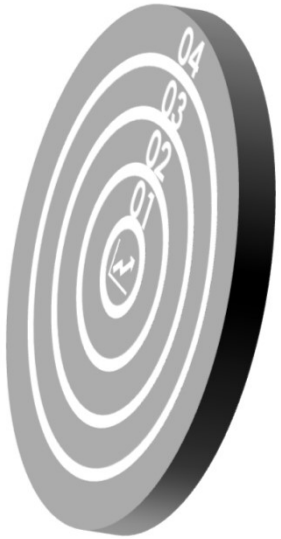


Very *scattered,* with many accessible and fragile attack surfaces

The growth of online account management and the increase in managed devices increases exposure by pushing more critical infrastructure to the *edge*

Significant amount of critical operational data transacted via SCADA channels (often unencrypted)

Critical infrastructure and personal data are very valuable to nation-state actors and the black markets



Large and Scattered Attack Surfaces

What is Cybersecurity?

Cybersecurity is the collection of tools, **policies**, security concepts, security safeguards, guidelines, risk management approaches, training, best practices, and technologies that can be used to protect the cyber environment and organization and user's assets.

Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

ITU-T X.1205, Overview of cybersecurity

Ransomware: Effective and Costly

Cybersecurity Ventures predicted ransomware damages topped $11.5 billion in 2018, up from $325 million in 2015, with attacks on business every 14 seconds.

Michigan utility paid $25,000 bounty to nation-state attackers to unencrypt systems

"The ransomware was delivered via a phishing attack and malicious attachments that locked them out of all their systems. The Lansing Board of Water & Light chose to pay $25,000 in bitcoin because it was cheaper than replacing all the infected computers and software, which would have cost up to $10 million. As it is, the incident cost them $2.5 million to wipe the infected computers and beef up their security controls, much of which was covered by insurance."

Phil Neray

Lake City, FL: $400,000
Riviera Beach, FL: $600,000
Key Biscayne, FL: TBD
Jackson County, GA: $400,000
Georgia Administrative Office of the Courts: TBD
Dekalb, IL: Under Investigation
City of Atlanta, GA: $52,000 Ransom, **$7.2 Million To Recover (So Far)**
City of Baltimore, MD: Ƀ75,000 per User, **$18 Million Damages (So Far)**
Fort Collins, CO – Loveland Water District
Jacksonville, NC - Onslow Water and Sewer Authority: Hit after Hurricane Florence

"Organizations must face a troubling fact: Defending their digital perimeter is not enough. They should assume that successful cyberattacks will occur—and develop an effective plan to mitigate the impact."

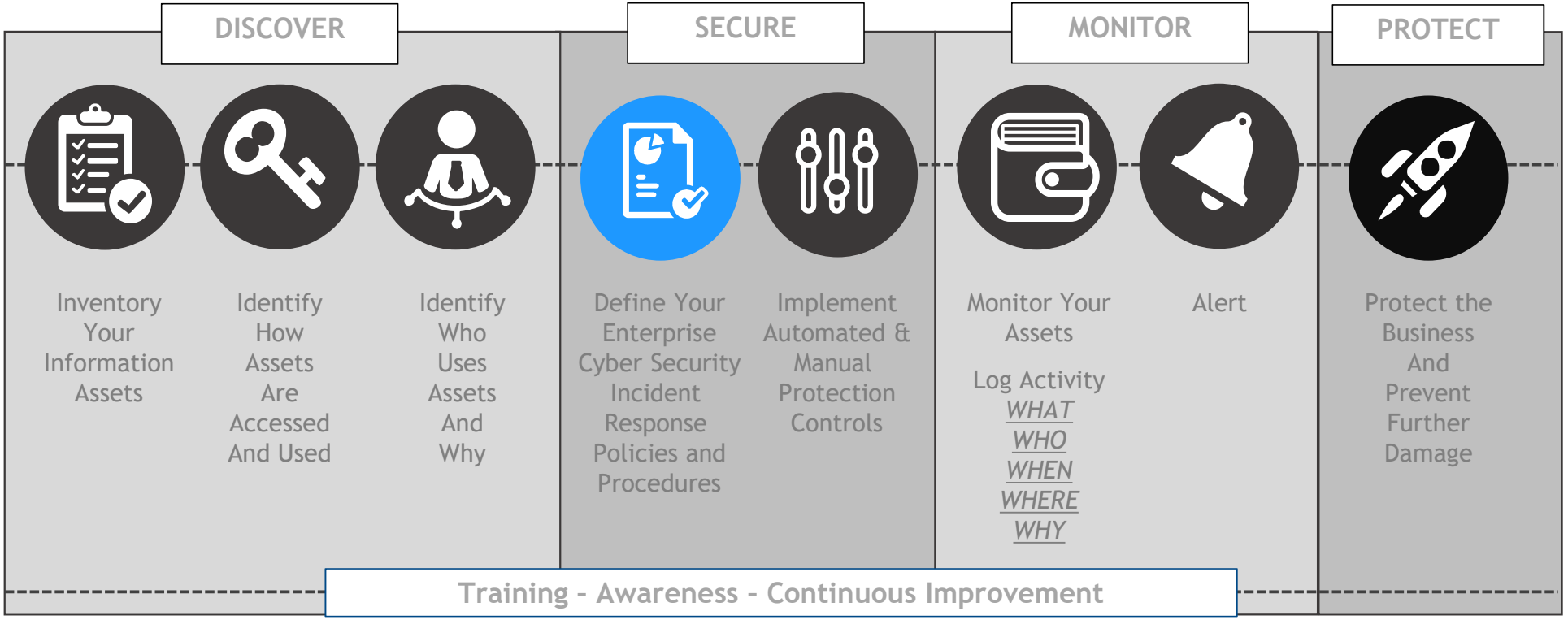
- McKinsey

AESI

Make Sure You Are Protected

Prepare Your Policy and Procedure Library

Cybersecurity Framework



E.O. 12977: Create a Risk Management Process for Critical Infrastructure

The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard Appendix A: The Design-Basis Threat (DBT) Report addresses:

- The threats, consequences and vulnerabilities of undesirable events that could compromise critical infrastructure;
- Physical security of federal facilities;
- Criteria and processes that those responsible for the security of critical infrastructure should use to determine an appropriate security level;
- An integrated, single source of security countermeasures;
- Customization of countermeasures based on the type of infrastructure being evaluated and protected.

Baseline Your Incident Response Program

The Interagency Security Committee Standard Appendix A: The Design-Basis Threat (DBT) Report prescribes six (6) incident response activities that are generally accepted as the foundation for a comprehensive incident management process.

Assemble Your Policy and Procedure Library and Supporting Artifacts

Preparation	Identification	Containment	Eradication	Recovery	Follow Up
• **Incident Response Plan** • Declaration Guide • Notification Plan • Reporting and Escalation Plan • Asset Inventory • User Profiles by Service • System and Data Backup/Recovery Plan • Run Books, SOPs by Service • Site Safety Response and Recovery Guide • Evidence Collection and Preservation Plan • Maintenance and Service Schedules	• **Incident Recognition and Identification Plan** • Abnormal Behavior Recognition Procedure [Baselines] • Classification Procedure [Declaration, Notification, Reporting and Escalation] • Incident Reporting Procedure	• Quarantine Procedure • Activation and Verification of Automated and Manual Controls • Trusted Connect Procedure • System State Backup and Restore Procedure	• Safe Startup and Shutdown Procedure • Systems Cleaning Procedure	• **Test Plan** • System and Data Recovery Procedure • System Integrity Check Procedure • Baseline Restore Procedure • Patch Management Procedure • System Rebuild Procedure • Password Management Procedure • File Integrity Check and Replacement Procedure • System Validation Procedure • Network Connect Procedure • Monitoring Restoration Procedure	• Incident Closeout Procedure • Evidence Chain of Custody Procedure • Legal and Regulatory Notifications

Assemble Your Policy and Procedure Library and Supporting Artifacts

Preparation

Preparation is an ongoing activity that links directly to your business operations. Not only are incident management policies and procedures developed and updated, asset inventories, user profiles, backup and restoration procedures, run books, SOPs and maintenance and service schedules should be continuously updated to ensure that you can recover all services to some known good point prior to the incident.

- Incident Response Plan
- Declaration Guide
- Notification Plan
- Reporting and Escalation Plan
- Asset Inventory
- User Profiles by Service
- System and Data Backup/Recovery Plan
- Run Books, SOPs by Service
- Site Safety Response and Recovery Guide
- Evidence Collection and Preservation Plan
- Maintenance and Service Schedules

Assemble Your Policy and Procedure Library and Supporting Artifacts
Identification

Preparation | **Identification** | Containment | Eradication | Recovery | Follow Up

Identification of threats or impacts often requires significant investigation to recognize that an incident has occurred and to determine the extent of any impacts.

An Incident Response Team can diagnose and triage an incident much faster when they know what "normal" service operations look like.

- Incident Recognition and Identification Plan
- Abnormal Behavior Recognition Procedure [Baselines]
- Classification Procedure [Declaration, Notification, Reporting and Escalation]
- Incident Reporting Procedure

Assemble Your Policy and Procedure Library and Supporting Artifacts

Containment

Rapid containment is critical to minimize service impacts. Once a threat is contained, temporary fixes may be applied to prevent the threat from re-emerging and to accelerate service restoration.

- Quarantine Procedure
- Activation and Verification of Automated and Manual Controls
- Trusted Connect Procedure
- System State Backup and Restore Procedure

Assemble Your Policy and Procedure Library and Supporting Artifacts

Eradication

Eradication may be as simple as applying a patch or as complex as re-imaging or rebuilding a complete system or service.

The primary goal is to close the vulnerabilities or entry points that were compromised to obtain access to the environment.

There is an argument that the IR team should also be documenting all actions required to eradicate the threat. In addition, any defenses in the network should be improved so that the same incident doesn't occur again.

- Safe Startup and Shutdown Procedure
- Systems Cleaning Procedure

Assemble Your Policy and Procedure Library and Supporting Artifacts

Recovery

Systems and data are restored to a know good point, and production service is resumed.

A comprehensive Test Plan can guide testing and verify that services are fully restored and operating as they should.

- Test Plan
- System and Data Recovery Procedure
- System Integrity Check Procedure
- Baseline Restore Procedure
- Patch Management Procedure
- System Rebuild Procedure
- Password Management Procedure
- File Integrity Check and Replacement Procedure
- System Validation Procedure
- Network Connect Procedure
- Monitoring Restoration Procedure

Assemble Your Policy and Procedure Library and Supporting Artifacts

Follow Up

Preparation | Identification | Containment | Eradication | Recovery | **Follow Up**

The final phase, Follow Up, includes collection and tagging of evidence, completion of an incident report, and final internal and external communications regarding the outcome of the incident response.

Incidents that cause significant impacts to service are, in certain cases, reportable to a regulator. Reportable events should be documented thoroughly and evidence retained to minimize the possibility of fines or other punitive actions.

Finally, lessons learned should be reviewed and applied to the Incident Response Plan so that future incidents may be less impactful.

- Incident Closeout Procedure
- Evidence Chain of Custody Procedure
- Legal and Regulatory Notifications

Considerations

- Integrate Incident Management with Business Continuity and Disaster Recovery Management
- Architect *Hot-Hot* infrastructure to reduce stranding assets and to facilitate rapid fail-over, where possible and practical
- Leverage CIP guidance, even if your utility isn't subject to NERC oversight
- Implement hardware-based point-to-point encryption where possible
- Limit, and disable where possible, access to the Internet and other untrusted networks
- Disallow remote access to SCADA environments
- Don't hold transient data that could be stolen or lost (cardholder data, SCADA transactional information, etc.)
- Maintain patches and updates on ALL software and operating systems
- Limit access to SCADA and customer systems to trusted and credentialed users, and revoke when not needed
- White list access to systems that transact controlled and confidential information
- Limit physical access to only authorized personnel
- Enforce policies regarding the physical repair and/or upgrade of all infrastructure
- Deploy security software (EPP, DLP, etc.) and automatically update with the latest signatures

Mark McKinney

Mark McKinney CISSP, CISA, CFE, CCFE
Director, Cybersecurity Services
AESI – US Inc.

E: markm@aesi-inc.com

T: 770.870.1630 x. 279