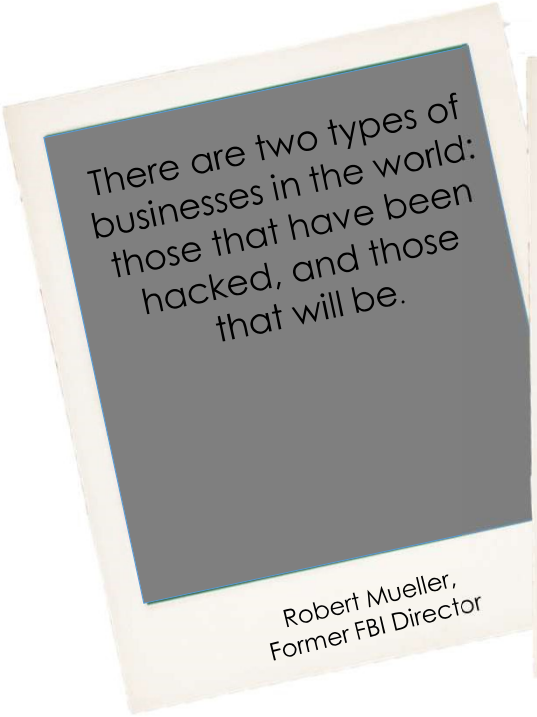
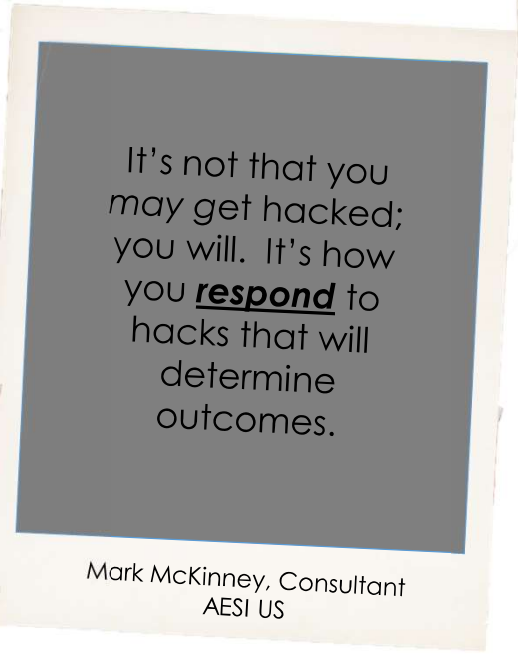
Southeast Regional Municipal Utility Cybersecurity Summit 2019

Framework for Good Cybersecurity Hygiene: The Importance of Incident Response

Mark McKinney MSIM, 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

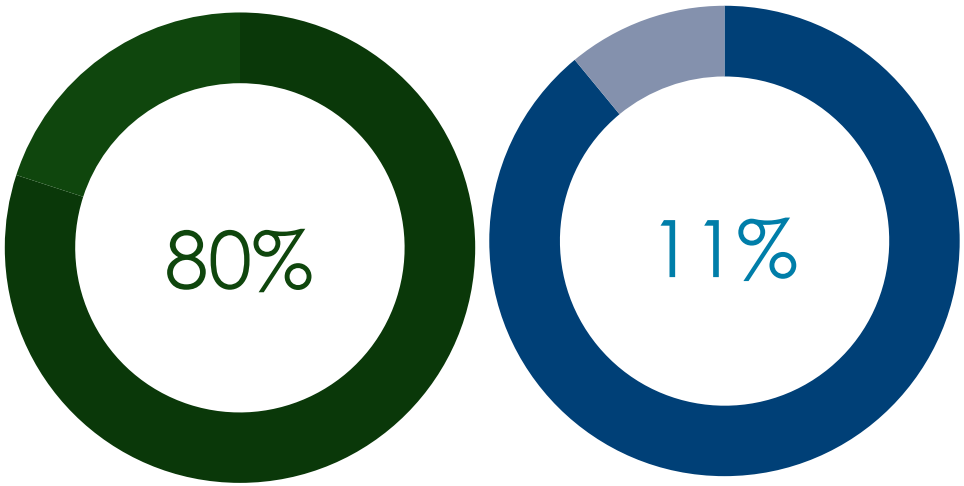
$6T	Estimated global cost of cyber crime expected to exceed $6T by 2021. Up from $3T in 2015, and $600B in 2014.
+30K	FBI Internet Crimes Complaint Center vetted 301,580 complaints in 2017, up from 269,422 in 2014. *4,063,933 since 2000*.
3000+	Estimated number of cyber attempts against U.S. energy sector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

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.

Trustwave 2018 Global Security Report



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."

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

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

Protecting Critical Infrastructure

Presidential Orders and Agency Directives

Executive Order 13636: Call for a Common Framework

Strengthen the security and resilience of the nation's critical infrastructure

Executive Order 13636, *"Improving Critical Infrastructure Cybersecurity"*

Presidential Policy Directive 21, *"Critical Infrastructure Security and Resilience"*

Executive Orders 13800 and 12977: Strengthen Federal Cybersecurity and Enhance Incident Coordination

Improve Response and Coordination to Cyber Security Incidents

United States Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

Presidential Policy Directive 41, *United States Cyber Incident Coordination*

Executive Order 12977 created the Interagency Security Committee to "…Improve government-wide coordination of security initiatives"

E.O. 13800 Federal Assessment

Required the Secretaries of Energy and Homeland Security to assess:

- Potential scope and duration of a prolonged power outage associated with a significant cyber incident;
- Readiness of the United States to manage the consequences of such an incident; and
- Gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident.

Assessment Findings

Identified Gaps

1. Situational Awareness and Incident Impact Analysis
2. Roles and responsibilities
3. Cybersecurity and Incident Response Integration into Cross-Functional Plans
4. Workforce Availability and Expertise
5. Supply Chain and Trusted Partners
6. Public-Private Cybersecurity Information Sharing
7. Resources for Cybersecurity Preparedness

A Comprehensive Approach

The assessment highlighted the need for

- A standardized risk-based approach to incident management designed to provide maximum visibility into the maturity and effectiveness of incident response and management procedures, and

- A comprehensive strategy that combines broad, enterprise reviews to validate that systemic risks and cross-functional integrations are addressed, and assurances that task areas are clearly identified and actionable.

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.

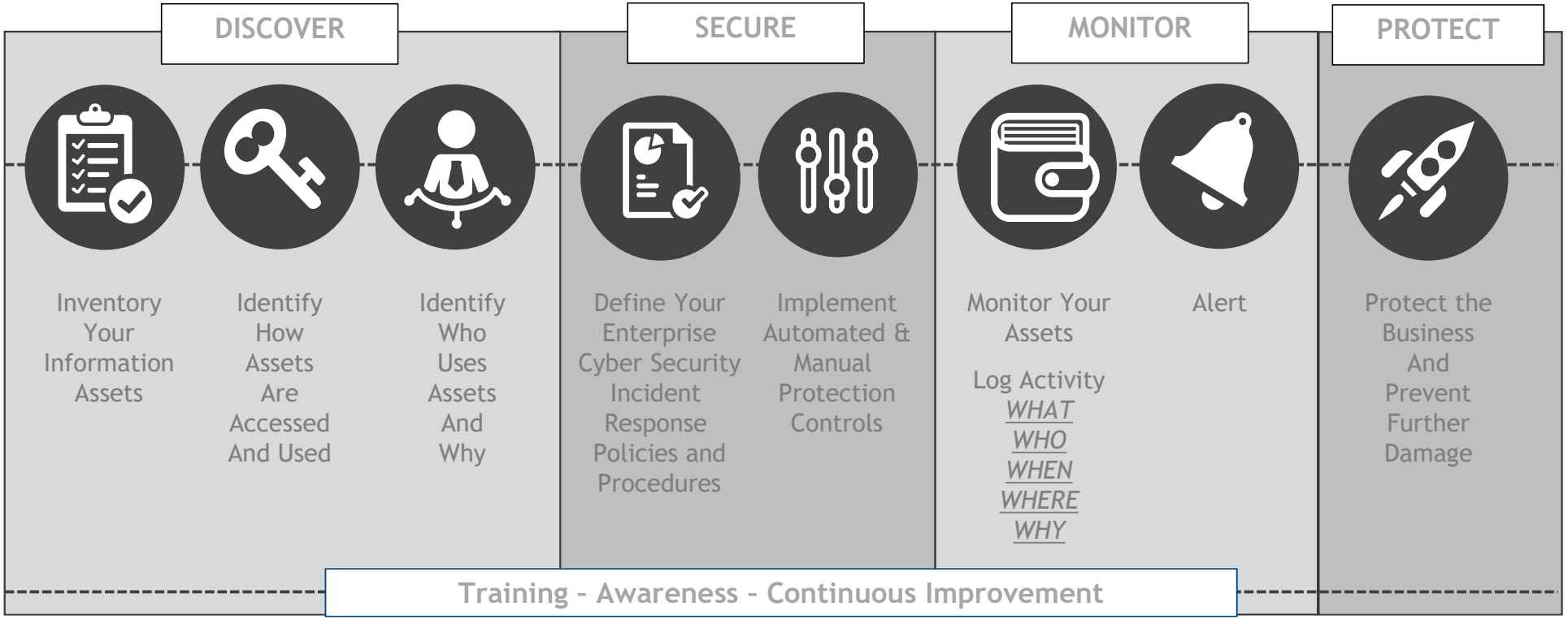
A Comprehensive Risk Management Process for Critical Infrastructure that Combines Cyber and Physical Security

Initially drafted to address physical security of federal facilities, the ISC standard combines with information found in DoDI (DoD Instruction) 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), which specifies a common set of security controls derived from NIST 800-53, assessment procedures derived from NIST SP 800-53A, and overlays with compliance values, implementation guidance, and assessment criteria defined in E.O. 12977 for Physical Security, into a comprehensive Risk Management Framework that provides the foundation to determine appropriate security levels and provide an integrated, single source of security countermeasures, and customization of countermeasures based on the type of infrastructure being evaluated and protected.

Make Sure You Are Ready

Design and Implement Effective Incident Management and Response Programs

Cybersecurity Framework



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.

Building An Incident Response Plan

Preparation: Have You Baselined Your Security Posture?

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

Key Activities Checklist

- Is your incident response plan current?
- When was the last time the plan was exercised?
- Are incident response policies, plans and procedures readily available to ALL employees and assigned IR team members? When were they reviewed and updated?
- Do you have an assigned incident response team, with clearly defined roles and responsibilities?
- Is there budget allocated?
- Is your IR team equipped with tools to quickly recognize, respond to and contain cyber incidents?

Policy and Procedure Checklist

- **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

Building An Incident Response Plan

Identification: Do You Know How to Recognize and Report an Incident?

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

Key Activities Checklist

- How are incident signatures recorded and preserved?
- Is evidence cataloged and preserved?
- Can normal operations continue or resume during an investigation?
- Does your organizations handle any privacy information that could be construed as personally identifiable information (PII)?
- Are procedures in place to enable customers to report anomalous activity or possible mis-use of PII?

Policy and Procedure Checklist

- Incident Recognition and Identification Plan (Master)
- Abnormal Behavior Recognition Procedure [Baselines]
- Incident Reporting Procedure [Escalation]

Building An Incident Response Plan

Identification: Do You Know How to Classify an Incident?

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

Impact Classifications	Impact Description
Functional Impact	HIGH – Organization has lost the ability to provide all critical services to all system users.
	MEDIUM – Organization has lost the ability to provide a critical service to a subset of system users.
	LOW – Organization has experienced a loss of efficiency, but can still provide all critical services to all users with minimal effect on performance.
	NONE – Organization has experienced no loss in ability to provide all services to all users.
Information Impact	CLASSIFIED – The confidentiality of classified information was compromised.
	PROPRIETARY – The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.
	PRIVACY – The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised.
	INTEGRITY – The necessary integrity of information was modified without authorization.
	NONE – No information was exfiltrated, modified, deleted, or otherwise compromised.
Recoverability	REGULAR – Time to recovery is predictable with existing resources.
	SUPPLEMENTED – Time to recovery is predictable with additional resources.
	EXTENDED – Time to recovery is unpredictable; additional resources and outside help are needed.
	NOT RECOVERABLE – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).
	NOT APPLICABLE – Incident does not require recovery.

NIST SP 800-61

Policy and Procedure Checklist

- Incident Recognition and Identification Plan (Master)
- Classification Procedure [Declaration, Notification]

Building An Incident Response Plan

Identification: Do You Understand Your Threat Landscape?

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

A threat vector, also called an attack vector, is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or commit a malicious act.

Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

Attack vectors may be aligned with events and incidents to develop appropriate triggers to fire alerts.

Threat Vector	Description	Example
Unknown	Cause of attack is unidentified.	This option is acceptable if cause (vector) is unknown upon initial report. The threat vector may be updated in a follow-up report.
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	Denial of Service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures.
Web	An attack executed from a website or web-based application.	Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware.
Email	An attack executed via an email message or attachment.	Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message.
External/Removable Media	An attack executed from removable media or a peripheral device.	Malicious code spreading onto a system from an infected USB flash drive.
Impersonation/Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute.	Spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization.	A misplaced laptop or mobile device.
Other	An attack does not fit into any other vector	

NIST SP 800-61

Building An Incident Response Plan

Containment: Do You Know How to Minimize Damage and Begin Clean Up?

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

Key Activities Checklist

- Are system baselines backed up?
- Are evidence preservation controls activated?
- Do you have a defined methodology for classifying risk (H, M, L) based on potential loss perspectives?
- What is the process for modifying classifications as new information emerges throughout the investigation?
- How are subsequent notifications handled?
- Is there executive ownership assigned for managing documentation and evidence control throughout the response?
- Are containment thresholds defined in advance of any incident to minimize the time to respond and contain the incident?

Policy and Procedure Checklist

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

Building An Incident Response Plan

Eradication: Do You Know How to Eliminate the Threat(s)?

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

Key Activities Checklist

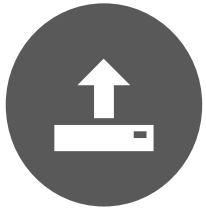
- Can systems be restored to a known good point from baseline backups?
- How is evidence chain-of-custody maintained during eradication?
- Is there assigned executive oversight of this process?
- What explicit authority is granted to the incident response team to:
  - Eradicate contaminants and recover services?
  - Rebuild an entire service?
  - Perform recovery operations - patch updates, restoring file systems, adding network filters, removing inappropriate software
  - Less intrusive activities?

Policy and Procedure Checklist

- Safe Startup and Shutdown Procedure
- Systems Cleaning Procedure

Building An Incident Response Plan

Recovery: Do You Know How to Resume "Normal" Operations?



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

Key Activities Checklist

- Are there defined uptime requirements for critical services?
- Are recovery plans available by service and/or application?
- Do recovery plans ensure service restoration within a required time threshold?
- Is there an approval process and time frame for procuring hardware or software? Does that coincide with your recovery time requirements?
- Is there any procurement authority granted to the incident response team that would not require executive approval?
- Is there an approval hierarchy in place to ensure continuity at the Manager through Executive levels?

Policy and Procedure Checklist

- 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

Building An Incident Response Plan

Follow Up: Do You Know How to Close Out an Incident Response?

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

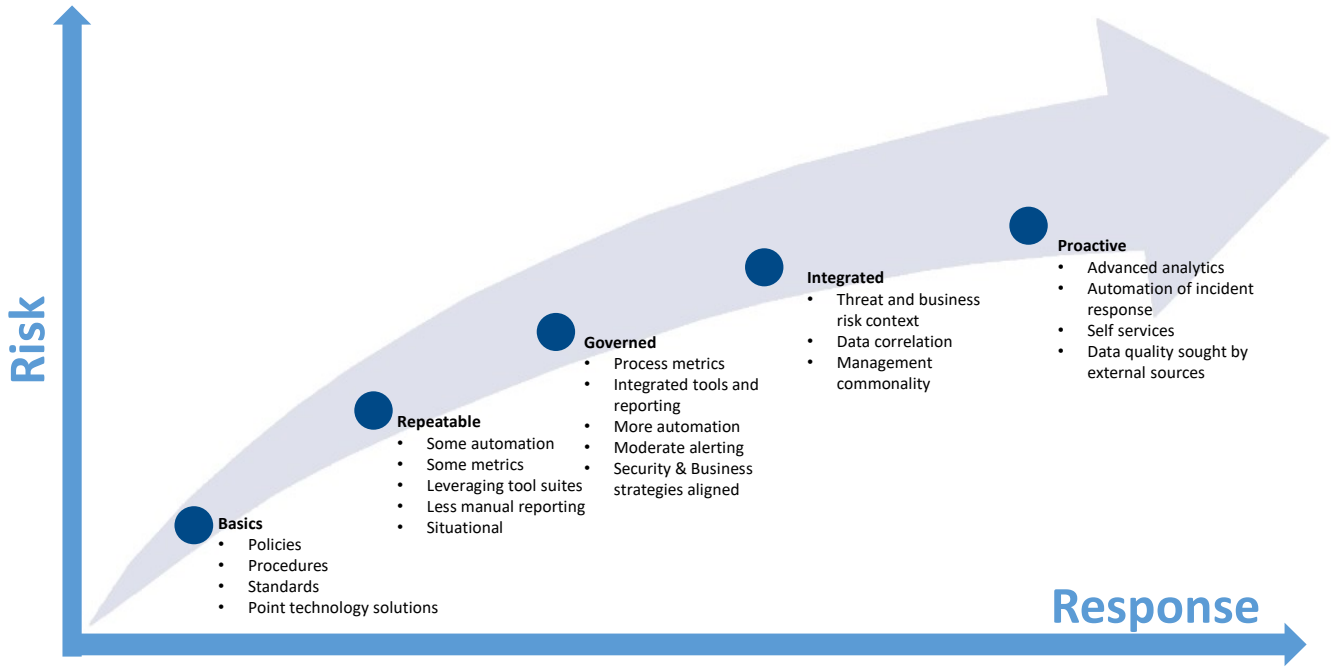
Key Activities Checklist

- Is someone assigned who Is responsible for managing and approving external communications related to the incident(s)?
- Is there legal representation to assist with legal or regulatory issues?
- How is evidence managed after the conclusion of the incident response?
- Who will manage the post-mortem activities and develop the plan-of-action (PoA) that addresses findings and any identified deficiencies related to the incident?
- How are final notifications handled?

Policy and Procedure Checklist

- Incident Closeout Procedure
- Evidence Chain of Custody Procedure

Continuously Improve Your Security Strategy



- Defensive
- Tactical
- Single event orientation
- Plan for known event types
- Retrospective metrics
- Minimal decision data

Offensive -
Strategic -
Contextual -
Mitigate unknown events -
Prospective Metrics -
Internal and External data awareness -

Checklist

- ❑ Assign an executive to take on responsibility for the plan and for integrating incident-response efforts across business units and geographies.
- ❑ Develop easily accessible quick-response guides for likely scenarios.
- ❑ Establish processes for making major decisions, such as when to isolate compromised areas of the network.
- ❑ Maintain relationships with key external stakeholders, such as law enforcement, breach-remediation providers and experts
- ❑ Ensure that documentation of response plans is available to the entire organization and is routinely refreshed.
- ❑ Ensure that all staff members understand their roles and responsibilities in the event of a cyber incident.
- ❑ Identify the individuals who are critical to incident response and ensure redundancy.
- ❑ Train, practice, and run simulated breaches to develop response routines. The best-prepared organizations routinely conduct *war games* to stress-test their plans, increasing awareness and fine-tuning response capabilities.

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