Intro

- Title:
  - "Cybersecurity Incident Response – It is More Than Just a Plan in the IT Department"
- Overview:
  - Incident Response is often treated as a plan or checklist that lives within the IT department that is utilized whenever alerts and alarm bells go off. In this session we'll take a look at the basics of incident response and then go beyond into the interconnected processes that make up and extend the Incident Response process such as roles and responsibilities (both identified and necessary), risk management (including third & fourth parties), logging and monitoring for event alerting, incident investigation and escalation, incident communication (notice), insurance considerations, and recovery & restoration resources. We'll also review and connect you with a checklist for broadening the discussion of Incident Response outside of the IT Department.
- This session will cover the following:
  - Recognize Incident Response as a Multifaceted Process
  - Participants will gain an appreciation for the multifaceted nature of incident response, moving beyond IT-centric views to understand the interconnected elements, roles, and responsibilities that comprise an effective response strategy.
  - Identify Key Components of Comprehensive Incident Response
  - Attendees will be able to identify critical interdependent components of incident response enabling them to evaluate and enhance their organization's readiness for incident response.
  - Enable Broader Incident Response Engagement
  - Attendees will be equipped to initiate discussions about incident response across various departments and industries, fostering a more inclusive and organization-wide approach to cybersecurity resilience.

weaver

Assurance • Tax • Advisory

Cybersecurity Incident Response – It is More Than Just a Plan in the IT Department

Agenda

- Challenge
- Event vs Incident
- What Do the Frameworks & Standards Say?
- Guidelines Outside of Controls
- Nuances
  - Roles & Responsibilities
  - Risk Mgmt – Third & Fourth Party
  - Logging & Monitoring
  - Incident Notices
- Tools And Resources
- Perspective & Next Steps
- Your Questions

Today's Presenter

WSET – Level 1
Chip and Dip Connoisseur
Dallas, TX – Native

Trip Hillman

CISSP, QSA, CISA, CEH, GPEN, GCFE, GSNA, GCWN, CCSK

Partner, Cybersecurity Services
Weaver
972.448.9276
Trip.Hillman@weaver.com

Trip Hillman
Partner, Cybersecurity Services at Weaver

Assumptions for this conversation:

*Have a **Corporate Network / Computer / Smartphone / Tablet***
***Use Data** – Data Base/Stores/Lake, Spreadsheets, Reports, etc.*
***Interact with Applications** – Internal Systems, Online SaaS Solutions, Vendor Solutions, APIs, etc.*
Expect Those Things to Work!

When I hear Incident Response I Feel…

OR

Challenge

We've Got a Plan & We *Think* it Works

Me: What Would You Do If *X* Happened?

Them: We'd call you…

- Frameworks, Standards, Compliance Regs
  - NIST-CSF, CIS-CSC
  - NIST 800-53, NIST 800-171, ISO 27001
  - PCI-DSS, DoD CMMC, NERC/FERC
- Industry/Trade Groups
- Insurance Providers
- Government Agency Guidance
  - DHS-CRR
  - Local State Requirements
- Vendor/Supplier Specifications

weaver
Assurance • Tax • Advisory

Cybersecurity Event vs Incident

Event

A cybersecurity event is a change in the normal behavior of a given system, process, environment or workflow.

Examples of a cybersecurity event:

- An employee flags a suspicious email
- Someone downloads software (authorized or unauthorized) to a company device
- A security lapse occurs due to a server outage

VS

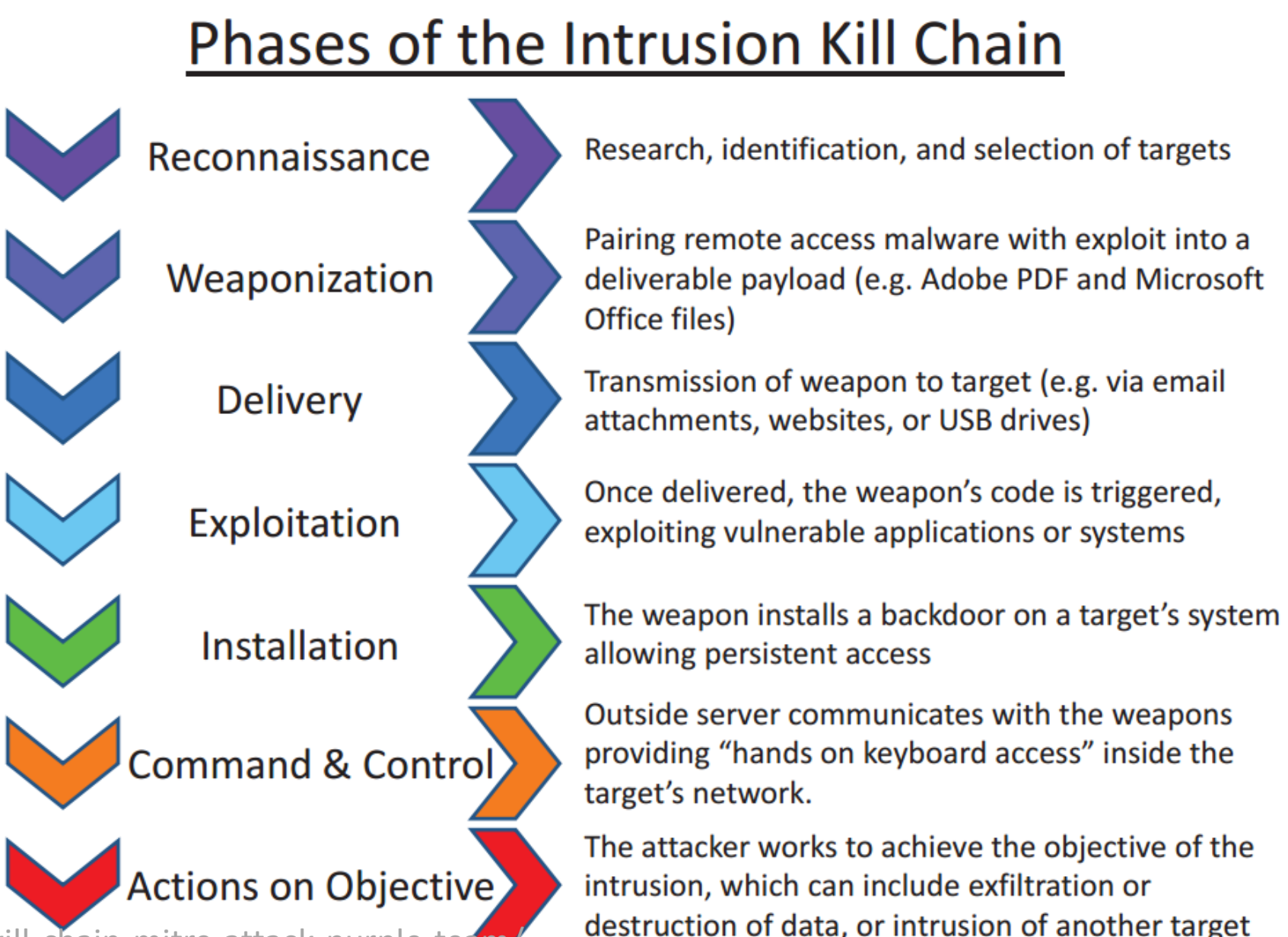
Incident

An incident is a change in a system that negatively impacts the organization, municipality, or business.

Examples of an incident:

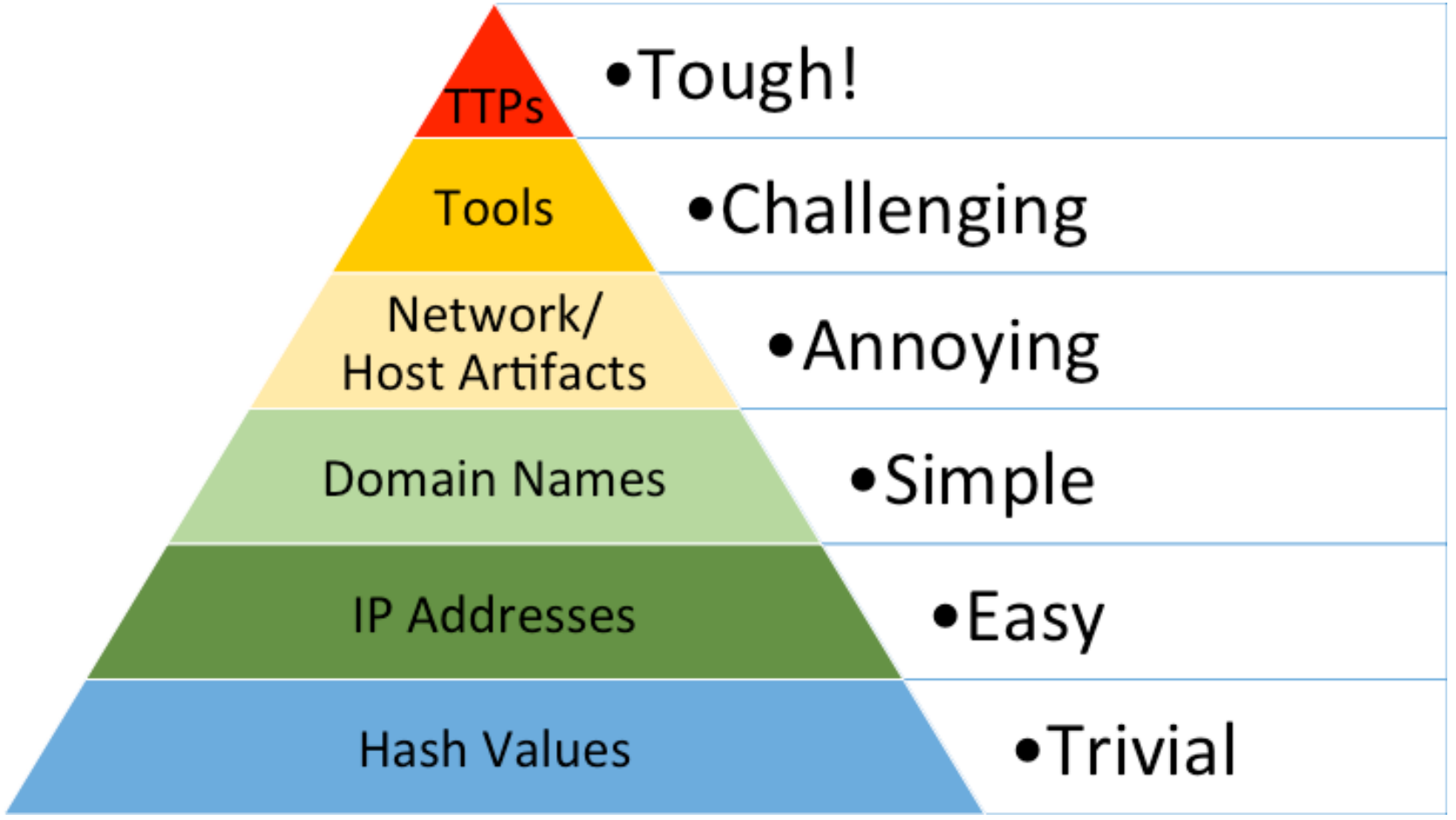
- An employee replies to a phishing email, divulging confidential information
- Equipment with stored sensitive data is stolen
- A password is compromised through a brute force attack on your system

Lockheed Martin Cyber Kill Chain



https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team/

Pyramid of Pain



https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team/

weaver
Assurance • Tax • Advisory

MITRE ATT&CK Framework

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration
51 items	27 items	49 items	18 items	17 items	17 items	25 items	13 items	9 items
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration
Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Data Compressed
AppCert DLLs	AppCert DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Browser Extensions	Data Encrypted
AppInit DLLs	AppInit DLLs	Clear Command History	Credential Dumping	Network Service Scanning	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Transfer Size Limits
Application Shimming	Application Shimming	Code Signing	Credentials in Files	Network Share Discovery	Logon Scripts	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol
Authentication Package	Bypass User Account Control	Component Firmware	Exploitation of Vulnerability	Peripheral Device Discovery	Pass the Hash	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Command and Control Channel
Bootkit	DLL Search Order Hijacking	Component Object Model Hijacking	Forced Authentication	Permission Groups Discovery	Pass the Ticket	InstallUtil	Data from Removable Media	Exfiltration Over Other Network Medium
Browser Extensions	Dylib Hijacking	Deobfuscate/Decode Files or Information	Hooking	Process Discovery	Remote Desktop Protocol	Launchctl	Data Staged	Exfiltration Over Physical Medium
Change Default File Association	Exploitation of Vulnerability	Disabling Security Tools	Input Capture	Query Registry	Remote File Copy	Local Job Scheduling	Email Collection	Scheduled Transfer
Component Firmware	Extra Window Memory Injection	DLL Search Order Hijacking	Input Prompt	Remote System Discovery	Remote Services	LSASS Driver	Input Capture	
Component Object Model Hijacking	File System Permissions Weakness	DLL Side-Loading	Keychain	Security Software Discovery	Replication Through Removable Media	Mshta	Man in the Browser	
Create Account	Hooking	Exploitation of Vulnerability	LLMNR/NBT-NS Poisoning	System Information Discovery	Shared Webroot	PowerShell	Screen Capture	
DLL Search Order Hijacking	Image File Execution Options Injection	Extra Window Memory Injection	Network Sniffing	System Network Configuration Discovery	SSH Hijacking	Regsvcs/Regasm	Video Capture	
Dylib Hijacking	Launch Daemon	File Deletion	Password Filter DLL	System Network Connections Discovery	Taint Shared Content	Regsvr32		
External Remote Services	New Service	File System Logical Offsets	Private Keys	System Owner/User Discovery	Third-party Software	Rundll32		
File System Permissions Weakness	Path Interception	Gatekeeper Bypass	Replication Through Removable Media		Windows Admin Shares	Scheduled Task		
Hidden Files and Directories	Plist Modification	Hidden Files and Directories	Securityd Memory		Windows Remote Management	Scripting		
Hooking	Port Monitors	Hidden Users	Two-Factor Authentication Interception			Service Execution		
Hypervisor		Hidden Window				Source		
Image File Execution		HISTCONTROL				Space after Filename		
		Image File Execution Options				Third-party Software		

T1015

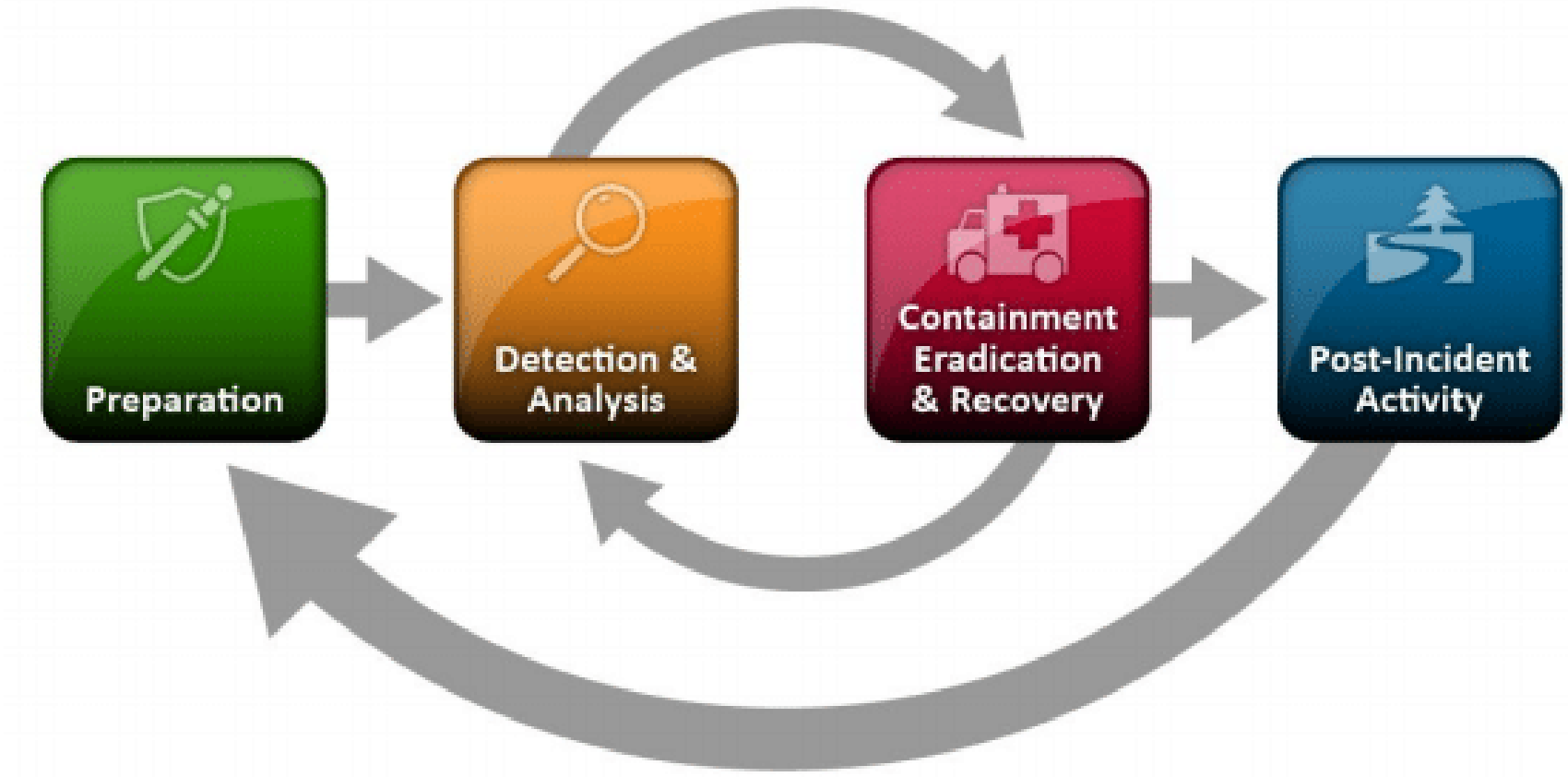
https://attack.mitre.org/

What Do The Frameworks Say?

- NIST 800-53r5 - Security and Privacy Controls for Information Systems and Organizations
- CIS CSC – Center for Internet Security Critical Security Controls
- NIST CSF – Cybersecurity Framework v2.0
- NIST 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- NIST 800-61r2 - Computer Security Incident Handling Guide

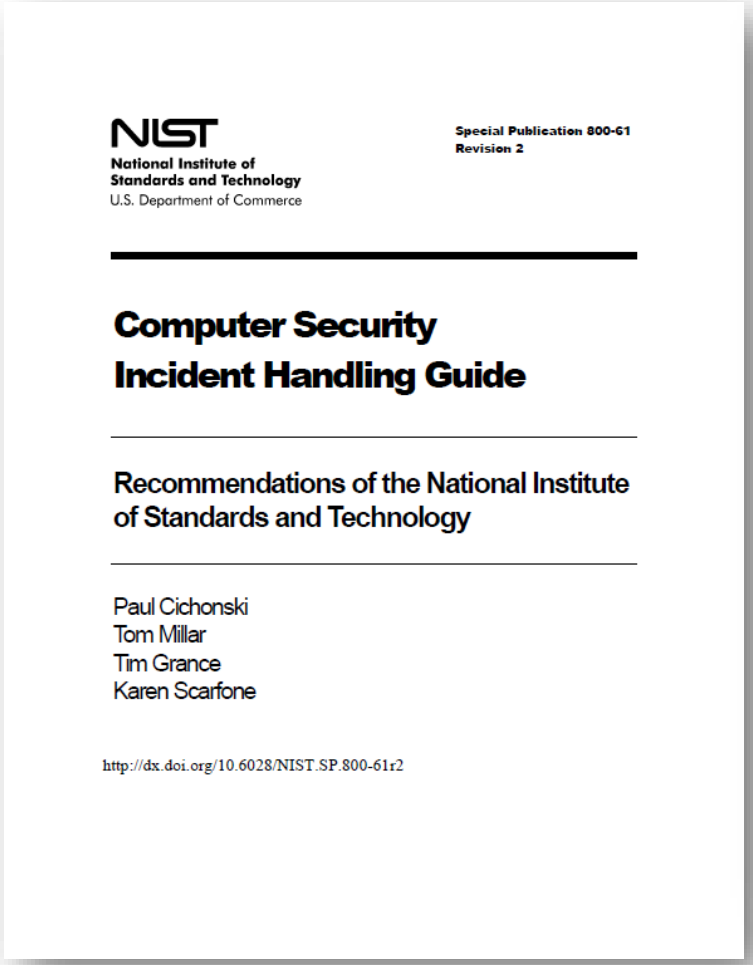
Largest Influence

- NIST 800-61r2
- 4 Major Phases
  - Preparation
  - Detection & Analysis
  - Containment Eradication & Recovery
  - Post-Incident Activity



NIST 800-61r2 – Computer Security Incident Handling Guide

- Incident Handling Checklist Included
- Value in the Appendix
  - » Appendix-A
    - 11 Scenarios
  - » Appendix-B
    - Types of Info to Collect
- Best Definitions
- And… It's Free



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

NIST 800-53r5

- IR-1: Policy and Procedures
- IR-2: Incident Response Training
- IR-3: Incident Response Testing
- **IR-4: Incident Handling**
- IR-5: Incident Monitoring
- IR-6: Incident Reporting
- IR-7: Incident Response Assistance
- IR-8: Incident Response Plan
- IR-9: Information Spillage Response

- Incident handling capability for incidents that is consistent with the incident response plan
  - includes preparation, detection and analysis, containment, eradication, and recovery
- Coordinate incident handling activities with contingency planning activities
- Incorporate lessons learned from
- Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization

IR-4(1): Automated Incident Handling Processes
IR-4(2): Dynamic Reconfiguration
IR-4(3): Continuity of Operations
IR-4(4): Information Correlation
IR-4(5): Automatic Disabling of System
IR-4(6): Insider Threats
IR-4(7): Insider Threats – Intra-organization Coordination
IR-4(8): Correlation with External Organizations
IR-4(9): Dynamic Response Capability
IR-4(10): Supply Chain Coordination
IR-4(11): Integrated Incident Response Team
IR-4(12): Malicious Code and Forensic Analysis
IR-4(13): Behavior Analysis
IR-4(14): Security Operations Center
IR-4(15): Public Relations and Reputation Repair

NIST CSF 2.0

National Institute of Standards and Technology (NIST) released the Cybersecurity Framework (CSF) 2.0 on February 26, 2024.

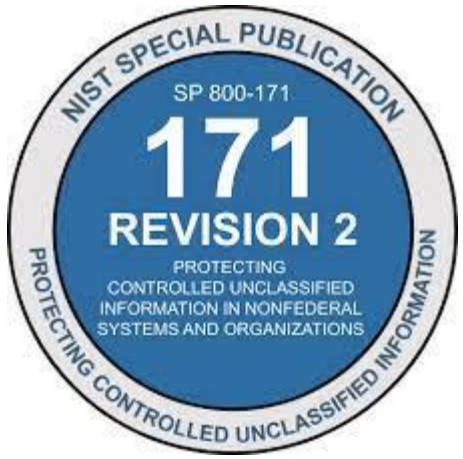
- RS.MA: Incident Management
  - **RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared**
  - RS.MA-02: Incident reports are triaged and validated
  - RS.MA-03: Incidents are categorized and prioritized
  - RS.MA-04: Incidents are escalated or elevated as needed
  - RS.MA-05: The criteria for initiating incident recovery are applied
- RS.AN: Incident Analysis
  - RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident
  - RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved
  - RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved
  - RS.AN-08: An incident's magnitude is estimated and validated
- RS.CO: Incident Response Reporting And Communication
  - RS.CO-02: Internal and external stakeholders are notified of incidents
  - RS.CO-03: Information is shared with designated internal and external stakeholders
- RS.MI: Incident Mitigation
  - RS.MI-01: Incidents are contained
  - RS.MI-02: Incidents are eradicated

weaver
Assurance • Tax • Advisory

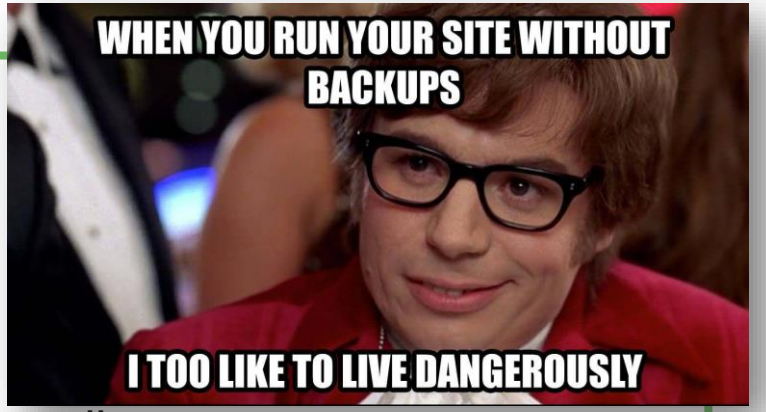
CIS CSC v8 - #17

- 17.1: Designate Personnel to Manage Incident Handling
- 17.2: Establish and Maintain Contact Information for Reporting Security Incidents
- 17.3: Establish and Maintain an Enterprise Process for Reporting Incidents
- 17.4: Establish and Maintain an Incident Response Process
- 17.5: Assign Key Roles and Responsibilities
- 17.6: Define Mechanisms for Communicating During Incident Response
- 17.7: Conduct Routine Incident Response Exercises
- 17.8: Conduct Post-Incident Reviews
- 17.9: Establish and Maintain Security Incident Thresholds

NIST 800-171r2



- 3.6.1: Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities
- 3.6.2: Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization
- 3.6.3: Test the organizational incident response capability



Common Issues Observed

- **Roles & Responsibilities** Not Granularly Defined
  - "We think we know who we need but we don't write it down"
  - "It's always going to be XYZ who handles that"
  - "Our **IT/Security function is outsourced** to ABC vendor who handles IR"
- **Lack of Logs** = Lack of Proof
  - Ironically the people that say "*we're not spending any more on storage?*" are also the people saying "*why can't we prove what happened?* "
  - API usage logs?
- "But we have **Cyber Insurance**…"
  - i.e. you probably have missing incident handling procedures
- "**Immutable**? I Don't Know But Our Backups are Encrypted"
  - Ransomware as a Service – Better 'Customer' Service but also Payment even more so **Doesn't** Equal Recovery Results
- **Third/Fourth Party** Considerations
  - "That's not our system though…"
  - "We have a contract / SLA in place"
  - Think MOVEit

Point of Reflections and Quick Wins

- Usable Contact Info – Readily Available
  - For Primary and Backup Employees
  - Critical Vendors/Service Providers
  - Legal Counsel
  - Insurance
- Dial the Numbers & Write the Text
  - Had a phone in the Ops Center that couldn't dial international numbers
- Meet with GC/Legal Today
  - What can you authorize, say, or do?
- Note Actions / Outcomes from Current IR TTX Exercises
  - You did the exercise, but what did you learn / improve

Incident Response Checklist for Non-IT Executives

Incident Response Checklist for Executives

How leaders can work with IT teams to help, not hurt, during a security incident

Ransomware attacks, Denial-of-Service attacks and data breaches are so disruptive, they are more than IT problems — when your company gets attacked, you need to know the plan. Your IT department's Incident Response Plan is only the starting point. How do CEOs, CFOs, COOs and other leaders support the IT team to help, and not hurt, as you get through the first 48 hours together?

As you fill in this checklist, a handy "In Case of Emergency" sheet at the end will record your key contacts and critical information. Share the finished page with other executives, general counsel and anyone else who will be part of the response.

Can your security incident response plan survive the first 24-48 hours?

- ☐ **Do we have an Incident Response Plan? Where is it stored? Who updates it? Does the plan offer different responses based on the type of threat? For example:**
  - How severe is the issue?
  - Is it an event (suspected, being investigated) or an incident (confirmed)?
  - Do response actions vary based on the type of threat? For example,
    - For ransomware threats, system integrity may take priority over availability
    - For insider threats, containment is usually the top priority

  Incident Response Plan file path: _____

  Incident Response Plan physical copy location: _____

  Date of last test/exercise of the Incident Response Plan: _____

- ☐ **Who is in charge, and who is their authorized backup?**
  - When there's an incident, who needs to know immediately?

    Cyber first responders: _____
  - Who is authorized to make decisions? _____
  - What authority does the IT response team have? (See "Preauthorized Response Actions" below.) _____
  - Who is the point person and IT liaison with top executives? _____
  - Who else is a key decision-maker for anything beyond the pre-agreed response authority? _____
  - Who is responsible for ensuring events and actions are documented? _____

- ☐ **Do we have cyber insurance?**
  - Who is authorized to initiate a claim with the insurance provider, and under what circumstances? (This decision requires an understanding of projected costs, claim limits, documentation requirements and impact on future premiums.) _____

  Are there insurance requirements that govern who you can hire as a response service provider, and if so, who? _____

  Cyber insurance carrier: _____

  Insurance contact: _____

- ☐ **Does the Incident Response team have well-documented pre-authorized response actions?**
  - What is the Incident Response team authorized to do without seeking executive permission?
    - Can they take a system or application offline? _____

      That requires understanding the impacts and potential workarounds:
      - What if it is a revenue-generating system?
      - What if it is the accounting system, payroll or time clock?
      - What if it affects critical operations for a customer?
    - Can they isolate a network segment (site, building, floor or department)? _____
    - Can they disable user(s) access? _____
    - Can they kick customers/users out of a system? _____
  - What can the Incident Response team be working on while waiting for a forensic response specialist? (Does the Incident Response Plan list basic triage steps?) _____

- ☐ **Do we have a plan for documenting the system's state of operations and managing proper chain of custody for evidence?**
  - **Does our plan specify what must be documented and how?** _____ In the heat of an incident, documenting actions can seem unimportant, but it's critical to record who did what and when. Putting a timeline together afterwards is extremely difficult. Good documentation can prove that IT responders acted promptly, and it helps recovery professionals as they come into or exit the response process.
  - **Has the plan been updated to account for service providers?** _____ Cloud Service Providers offer services at scale but that also means your response must scale as well. Do you have authorization to capture all necessary artifacts?
  - **Who is assigned** to make sure actions and a timeline are recorded? _____

In Case of Cyber Emergency:

Fill this out and share with executives, general counsel, public information/ PR contacts and others who might need to assist in a cyber response:

Our Incident Response Plan is located here:

File path: _____

Physical copies: _____

Date of last Incident Response Plan exercise/test: _____

Our cyber first responders are: _____

Our response authorized decision-makers are: _____

Our cyber insurance carrier is: _____

Contact name and phone: _____

Our incident communication lead is: _____

Other things to know: _____

To learn more about how Weaver can help you improve or manage cybersecurity, visit https://weaver.com/services/cybersecurity.

Cyber Placemat

weaver
Assurance • Tax • Advisory

Program & Control Frameworks
- ❑ NIST 800-53
- ❑ CIS CSC
- ❑ NIST CSF
- ❑ ISO 27001
- ❑ CSA CCM

Compliance Requirements
- ❑ 800-171
- ❑ CMMC
- ❑ PCI-DSS
- ❑ HIPAA
- ❑ NERC / FERC
- ❑ FFIEC
- ❑ FISMA
- ❑ FedRAMP

Additional Guidance
- ❑ DHS CPG
- ❑ DHS CRR
- ❑ MITRE ATT&CK
- ❑ MITRE D3FEND
- ❑ MITRE ENGAGE

Organization Overview:
- ❑ Name: _____
- ❑ Mission: _____
- ❑ Goals: _____
- ❑ Purpose: _____
- ❑ Strategy/Vision: _____
- ❑ Values: _____

Purpose of the System:

_____

Objectives & Features:

_____

Critical Roles & Responsibilities:

_____

Stakeholders:

External
- ❑ Citizens/Customers: _____
- ❑ Regulators: _____
- ❑ Legal Counsel: _____
- ❑ Consultants: _____
- ❑ Service Providers: _____

Internal
- ❑ Governance Board: _____
- ❑ Executive Leadership: _____
- ❑ Management Team: _____
- ❑ Technical Specialists: _____
- ❑ Information Owner: _____
- ❑ System Owner: _____
- ❑ System Security Officer: _____

Types of data Handled:
- ❑ Employee PII
  - ☐Stored ☐Processed ☐Transmitted
- ❑ Users/Citizen/Constituent/Student/Customer PII
  - ☐Stored ☐Processed ☐Transmitted
- ❑ Sensitive / Classified Data
  - ☐Stored ☐Processed ☐Transmitted
- ❑ Financial Data
  - ☐Stored ☐Processed ☐Transmitted
- ❑ Payment/Credit Card Data
  - ☐Stored ☐Processed ☐Transmitted
- ❑ Health/Medical Data
  - ☐Stored ☐Processed ☐Transmitted
- ❑ Legal/CJIS Data
  - ☐Stored ☐Processed ☐Transmitted
- ❑ Compliance/Regulatory Data
  - ☐Stored ☐Processed ☐Transmitted
- ❑ GIS Data
  - ☐Stored ☐Processed ☐Transmitted
- ❑ Environmental/Natural Resource Data
  - ☐Stored ☐Processed ☐Transmitted
- ❑ Other: _____
  - ☐Stored ☐Processed ☐Transmitted
- ❑ Other: _____
  - ☐Stored ☐Processed ☐Transmitted
- ❑ Other: _____
  - ☐Stored ☐Processed ☐Transmitted
- ❑ Other: _____
  - ☐Stored ☐Processed ☐Transmitted
- ❑ Other: _____
  - ☐Stored ☐Processed ☐Transmitted

How We Define a Technology Asset:

_____

How Would We Rate Our Technology Asset Inventory

☐ Comprehensive ☐ Incomplete

Systems & Connected Resources:
- ❑ Resources
  - ❑ Cloud/Shared
    - ☐IaaS ☐PaaS ☐SaaS ☐FaaS
    - ☐On-Prem ☐Co-located ☐Hosted
- ❑ Application 1: _____
  - ❑ Component Inventory Location: _____
  - ❑ Responsible Personnel: _____
- ❑ Application 2: _____
  - ❑ Component Inventory Location: _____
  - ❑ Responsible Personnel: _____
- ❑ Application 3: _____
  - ❑ Component Inventory Location: _____
  - ❑ Responsible Personnel: _____
- ❑ Storage Locations not Inventoried with Application
  - ❑ Cloud Storage: _____
  - ❑ Database: _____
  - ❑ Network/Fileshare: _____
  - ❑ Cache Locations: _____
  - ❑ Log Locations: _____
  - ❑ Backup Locations: _____

Note: Separately referenced application inventories should include all system components including hardware device type, Serial #, OS Version, Software version(s), and libraries.

Shared Systems & Processes:
- ❑ HR Systems
- ❑ ERP & Financial Systems
  - ❑ Billing/Invoicing
  - ❑ Time/Expense Entry
- ❑ Contract Systems
- ❑ CRM
- ❑ Identity Systems
  - ❑ LDAP/Active Directory
  - ❑ Cloud Access Security Broker
    - ❑ Okta
    - ❑ Duo
    - ❑ Ping
    - ❑ Other
  - ❑ Privileged Access Management

Key Devices (IT / OT):
- ❑ Servers
- ❑ Workstations
  - ❑ Desktops
  - ❑ Laptops
  - ❑ VDI/Thin Clients
- ❑ Mobile Devices
  - ❑ Smart Phones
  - ❑ Tablets
  - ❑ IOT
- ❑ Network Components
  - ❑ Firewall
  - ❑ Load Balancer
- ❑ Security Appliances
  - ❑ XYZ
- ❑ Hosted / Cloud
  - ❑ XYZ
- ❑ Connections / APIs
  - ❑ XYZ
  - ❑ XYZ
  - ❑ XYZ
- ❑ Other Component

Key Cybersecurity Program Attributes:
- ❑ Tools: _____
- ❑ Personnel: _____
- ❑ Processes: _____

weaver
Assurance • Tax • Advisory

Download for Resources

SCAN ME

Incident Response Checklist for Executives

How leaders can work with IT teams to help, not hurt, during a security incident

Ransomware attacks, Denial-of-Service attacks and data breaches are so disruptive, they are more than IT problems — when your company gets attacked, you need to know the plan. Your IT department's Incident Response Plan is only the starting point. How do CEOs, CFOs, COOs and other leaders support the IT team to help, and not hurt, as you get through the first 48 hours together?

As you fill in this checklist, a handy "In Case of Emergency" sheet at the end will record your key contacts and critical information. Share the finished page with other executives, general counsel and anyone else who will be part of the response.

Can your security incident response plan survive the first 24-48 hours?

- ☐ Do we have an Incident Response Plan? Where is it stored? Who updates it?
  Does the plan offer different responses based on the type of threat? For example:
  - How severe is the issue?
  - Is it an event (suspected, being investigated) or an incident (confirmed)?
  - Do response actions vary based on the type of threat? For example,
    - For ransomware threats, system integrity may take priority over availability
    - For insider threats, containment is usually the top priority

  Incident Response Plan file path: _____
  Incident Response Plan physical copy location: _____
  Date of last test/exercise of the Incident Response Plan: _____
- ☐ Who is in charge, and who is their authorized backup?
  - When there's an incident, who needs to know immediately?
    Cyber first responders: _____
  - Who is authorized to make decisions? _____
  - What authority does the IT response team have? (See "Preauthorized Response Actions" below.) _____
  - Who is the point person and IT liaison with top executives? _____
  - Who else is a key decision-maker for anything beyond the pre-agreed response authority? _____
  - Who is responsible for ensuring events and actions are documented? _____

- ☐ Do we have cyber insurance?
  - Who is authorized to initiate a claim with the insurance provider, and under what circumstances? (This decision requires an understanding of projected costs, claim limits, documentation requirements and impact on future premiums.) _____
  - Are there insurance requirements that govern who you can hire as a response service provider, and if so, who? _____
  - Cyber insurance carrier: _____
  - Insurance contact: _____
- ☐ Does the Incident Response team have well-documented pre-authorized response actions?
  - What is the Incident Response team authorized to do without seeking executive permission?
    - Can they take a system or application offline?
      That requires understanding the impacts and potential workarounds:
      - What if it is a revenue-generating system?
      - What if it is the accounting system, payroll or time clock?
      - What if it affects critical operations for a customer?
    - Can they isolate a network segment (site, building, floor or department)? _____
    - Can they disable user(s) access? _____
    - Can they kick customers/users out of a system? _____
  - What can the Incident Response team be working on while waiting for a forensic response specialist? (Does the Incident Response Plan list basic triage steps?) _____
- ☐ Do we have a plan for documenting the system's state of operations and managing proper chain of custody for evidence?
  - Does our plan specify what must be documented and how? _____
    In the heat of an incident, documenting actions can seem unimportant, but it's critical to record who did what and when. Putting a timeline together afterwards is extremely difficult. Good documentation can prove that IT responders acted promptly, and it helps recovery professionals as they come into or exit the response process.
  - Has the plan been updated to account for service providers? _____
    Cloud Service Providers offer services at scale but that also means your response must scale as well. Do you have authorization to capture all necessary artifacts?
  - Who is assigned to make sure actions and a timeline are recorded? _____

In Case of Cyber Emergency:

Fill this out and share with executives, general counsel, public information/PR contacts and others who might need to assist in a cyber response:

Our Incident Response Plan is located here:

File path: _____

Physical copies: _____

Date of last Incident Response Plan exercise/test: _____

Our cyber first responders are: _____

Our response authorized decision-makers are: _____

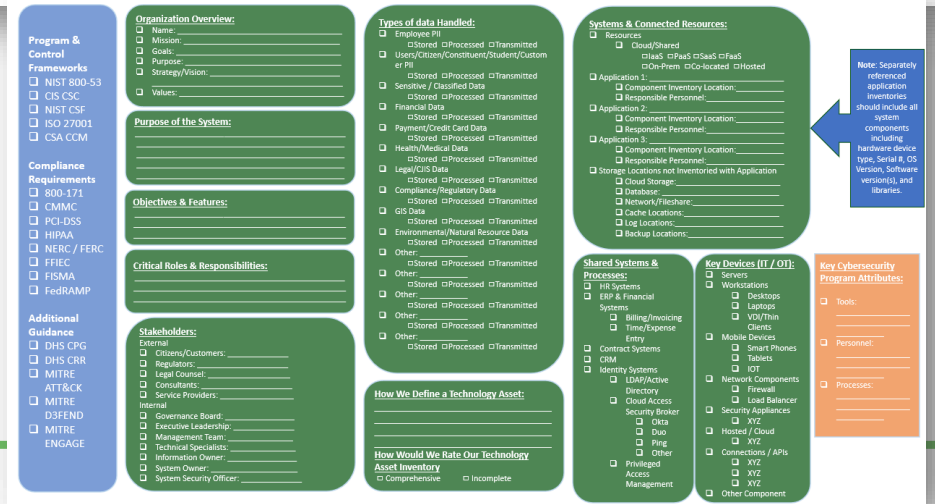
Our cyber insurance carrier is: _____

Contact name and phone: _____

Our incident communication lead is: _____

Other things to know: _____

To learn more about how Weaver can help you improve or manage cybersecurity, visit https://weaver.com/services/cybersecurity



Program & Control Frameworks
- ☐ NIST 800-53
- ☐ CIS CSC
- ☐ NIST CSF
- ☐ ISO 27001
- ☐ CSA CCM

Compliance Requirements
- ☐ 800-171
- ☐ CMMC
- ☐ PCI-DSS
- ☐ HIPAA
- ☐ NERC / FERC
- ☐ FFIEC
- ☐ FISMA
- ☐ FedRAMP

Additional Guidance
- ☐ DHS CPG
- ☐ DHS CRR
- ☐ MITRE ATT&CK
- ☐ MITRE D3FEND
- ☐ MITRE ENGAGE

Organization Overview:
- ☐ Name: _____
- ☐ Mission: _____
- ☐ Goals: _____
- ☐ Purpose: _____
- ☐ Strategy/Vision: _____
- ☐ Values: _____

Purpose of the System:

Objectives & Features:

Critical Roles & Responsibilities:

Stakeholders:
External
- ☐ Citizens/Customers: _____
- ☐ Regulators: _____
- ☐ Legal Counsel: _____
- ☐ Consultants: _____
- ☐ Service Providers: _____

Internal
- ☐ Governance Board: _____
- ☐ Executive Leadership: _____
- ☐ Management Team: _____
- ☐ Technical Specialists: _____
- ☐ Information Owner: _____
- ☐ System Owner: _____
- ☐ System Security Officer: _____

Types of data Handled:
- ☐ Employee PII ☐Stored ☐Processed ☐Transmitted
- ☐ Users/Citizen/Constituent/Student/Customer PII ☐Stored ☐Processed ☐Transmitted
- ☐ Sensitive / Classified Data ☐Stored ☐Processed ☐Transmitted
- ☐ Financial Data ☐Stored ☐Processed ☐Transmitted
- ☐ Payment/Credit Card Data ☐Stored ☐Processed ☐Transmitted
- ☐ Health/Medical Data ☐Stored ☐Processed ☐Transmitted
- ☐ Legal/CUI Data ☐Stored ☐Processed ☐Transmitted
- ☐ Compliance/Regulatory Data ☐Stored ☐Processed ☐Transmitted
- ☐ GIS Data ☐Stored ☐Processed ☐Transmitted
- ☐ Environmental/Natural Resource Data ☐Stored ☐Processed ☐Transmitted
- ☐ Other: _____ ☐Stored ☐Processed ☐Transmitted
- ☐ Other: _____ ☐Stored ☐Processed ☐Transmitted
- ☐ Other: _____ ☐Stored ☐Processed ☐Transmitted
- ☐ Other: _____ ☐Stored ☐Processed ☐Transmitted
- ☐ Other: _____ ☐Stored ☐Processed ☐Transmitted

How We Define a Technology Asset:

How Would We Rate Our Technology Asset Inventory
☐ Comprehensive ☐ Incomplete

Systems & Connected Resources:
- ☐ Resources
  - ☐ Cloud/Shared ☐IaaS ☐PaaS ☐SaaS ☐FaaS ☐On-Prem ☐Co-located ☐Hosted
- ☐ Application 1: _____
  - ☐ Component Inventory Location: _____
  - ☐ Responsible Personnel: _____
- ☐ Application 2: _____
  - ☐ Component Inventory Location: _____
  - ☐ Responsible Personnel: _____
- ☐ Application 3: _____
  - ☐ Component Inventory Location: _____
  - ☐ Responsible Personnel: _____
- ☐ Storage Locations not Inventoried with Application
  - ☐ Cloud Storage: _____
  - ☐ Database: _____
  - ☐ Network/Fileshare: _____
  - ☐ Cache Locations: _____
  - ☐ Log Locations: _____
  - ☐ Backup Locations: _____

Note: Separately referenced application inventories should include all system components including hardware device type, Serial #, OS Version, Software version(s), and libraries.

Shared Systems & Processes:
- ☐ HR Systems
- ☐ ERP & Financial Systems
  - ☐ Billing/Invoicing
  - ☐ Time/Expense Entry
- ☐ Contract Systems
- ☐ CRM
- ☐ Identity Systems
  - ☐ LDAP/Active Directory
  - ☐ Cloud Access Security Broker
    - ☐ Okta
    - ☐ Duo
    - ☐ Ping
    - ☐ Other
  - ☐ Privileged Access Management

Key Devices (IT / OT):
- ☐ Servers
- ☐ Workstations
  - ☐ Desktops
  - ☐ Laptops
  - ☐ VDI/Thin Clients
- ☐ Mobile Devices
  - ☐ Smart Phones
  - ☐ Tablets
  - ☐ IOT
- ☐ Network Components
  - ☐ Firewall
  - ☐ Load Balancer
- ☐ Security Appliances
  - ☐ XYZ
- ☐ Hosted / Cloud
  - ☐ XYZ
- ☐ Connections / APIs
  - ☐ XYZ
  - ☐ XYZ
  - ☐ XYZ
- ☐ Other Component

Key Cybersecurity Program Attributes:
- ☐ Tools: _____
- ☐ Personnel: _____
- ☐ Processes: _____

Cyber Audit Universe

NOTE: These are considerations only and the decision and ownership is dependent on the environment and risk management.

Year 1

- **Foundational**
  - Cybersecurity Program
  - Risk Assessment
  - Plan / Strategy Roadmap
  - Policy Review
- **Core**
  - Asset Management Inventory
  - Vulnerability Management
  - Vendor Management
  - IAM
    - Account Management
    - Multi-Factor Authentication

Year 2

- **Configuration Management**
  - Patch management
- **Logging and Monitoring**
  - Log sources
  - Detection capabilities
  - Existing Alerts
  - Investigation / Triage
- **Backup & Recovery**
  - Business Continuity Plan / Disaster Recovery
  - Ransomware
- **Incident Response**
- **App/Service Security**
  - Development (SDLC/DevOps)
  - API Security
  - Code Repository Management
  - Threat modeling

Year 3

- **Cyber Insurance**
- **Board Communication**
- **Third and Fourth Party Risk Management**
- **Mobile Device Management**
- **Mergers and Acquisitions**
- **Physical Security**

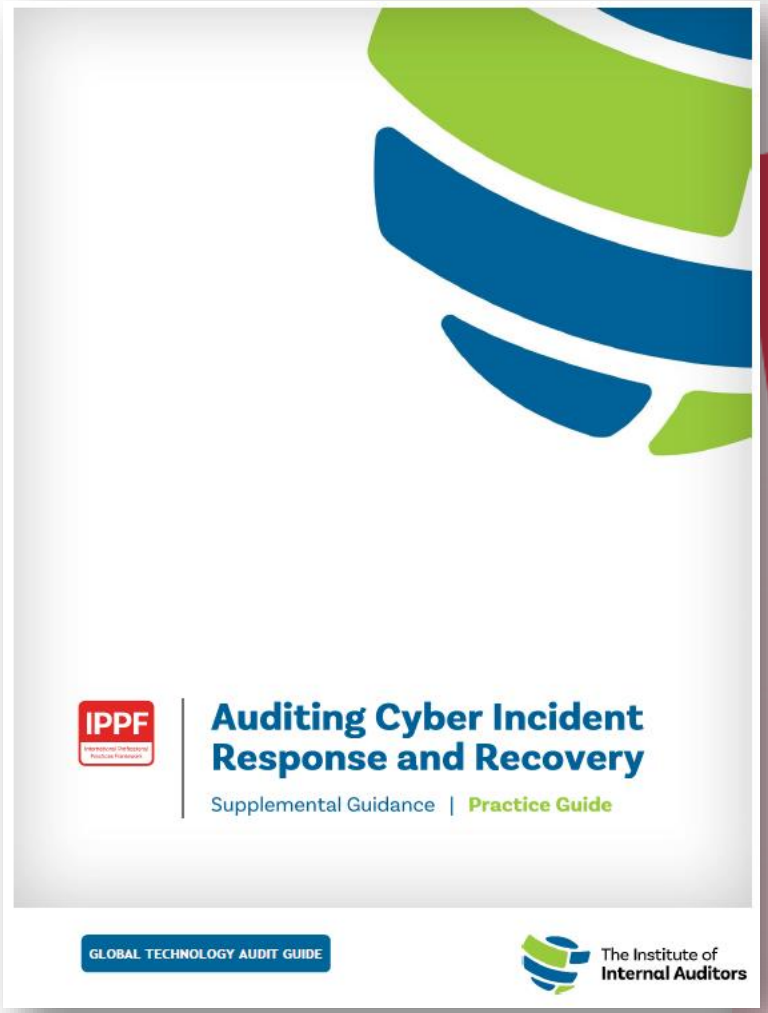
For Consideration

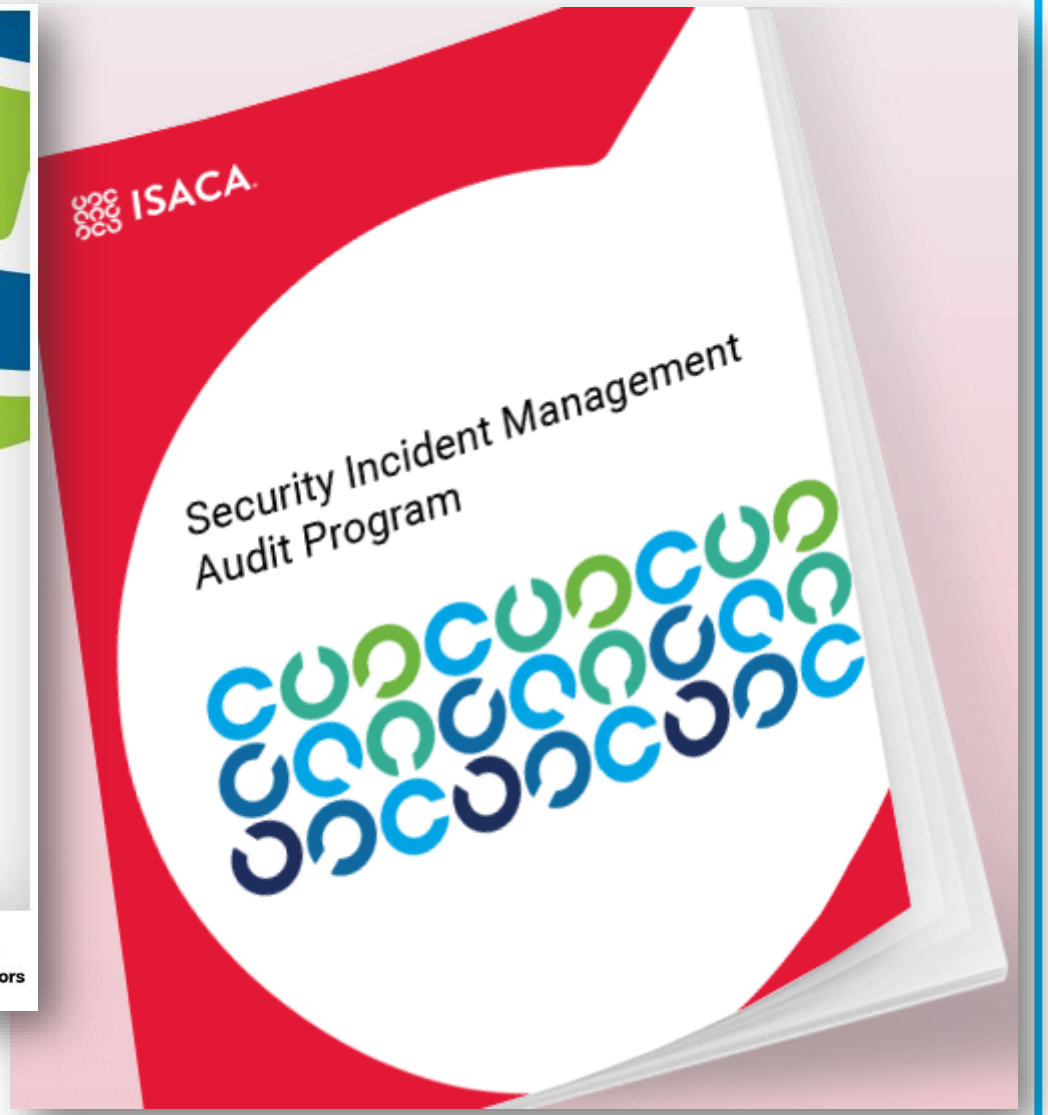
- **Leadership**
  - Staffing & Resources
  - Skills/Capabilities
    - IT/Infosec Training
- **Software Development Lifecycle**
- **Secure Network Design/Architecture**
- **Endpoint Detection and Response**
  - Email Security
- **Security Awareness Training**
  - Phishing exercises
- **Penetration Testing**

Cyber Program Perspective

Local Resource

- IIA GTAG
  - Auditing Cyber Incident Response & Recovery
- ISACA
  - Security Incident Management Audit Program





- NIST CSF (Cybersecurity Framework) Integration
  - » https://csrc.nist.gov/publications/detail/nistir/8374/draft
- Associated Audit Topics
  - » Incident Response
  - » Detection & Monitoring
  - » Recovery (BCP/DR)
  - » Threat/Risk Asmt.

https://csrc.nist.gov/publications/detail/nistir/8374/draft

weaver

Assurance • Tax • Advisory

Trip Hillman

CISSP, QSA, GPEN, GSNA, GCWN, GCFE, CEH, CCSK

Partner, Cybersecurity Services

Trip.Hillman@Weaver.com

972.448.9276


weaver
Assurance • Tax • Advisory

Common Questions Asked "For a Friend"

- How often do we need to organize a table top exercise? And who needs to be involved?
- If IT functions are outsourced to a service provider, who own's the Incident Response function?
- What in Incident Response has surprised you the most?
- What are the leading regulatory "gotcha's" for incident response?

Polling Question #1

Does your organization have a cybersecurity incident response plan?

- A) Yes – And it would work for cyber incidents from the news
- B) Yes – But it wouldn't work for cyber incidents from the news
- C) No – But we'll have one shortly after this talk
- D) Unsure – But I'm looking through the files now
- E) I'm legally bound from talking about this based on a prior issue that may or may not have happened

Polling Question #2

Do you test/validate your incident response plan at least annually with responders *and* executives?

- A) Yes, at least annually
- B) Yes, but greater than a year ago
- C) No, but it is on the plan now!
- D) No, we're all good
- E) Unsure

Polling Question #3

Do you leverage the MITRE ATT&CK framework in your environment?

- A) Yes
- B) No
- C) Unsure