Cybersecurity Incident Response Plans

October 12, 2023

TLP:CLEAR, ID# *202310121300*

Agenda

- National Institute of Standards and Technology (NIST)
- NIST Incident Response Framework
- NIST Special Publication 800-61
- What Is an Incident Response Plan?
- The Incident Response Lifecycle
- Incident Response Teams
- Scenario Walkthrough
- Why You Should Have an IRP
- Resources
- Questions

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

National Institute of Standards and Technology (NIST)

NIST Background

The National Institute of Standards and Technology is a prestigious institution in the United States that fosters scientific research, technological innovation, and the establishment of standards.

- Established in 1901 as the National Bureau of Standards (NBS)
- One of the oldest physical science laboratories
- Initially tasked with ensuring uniformity standards
- Used to publish consumer guides
- Expanded into broader scientific research
- Renamed the National Institute of Standards and Technology in 1988

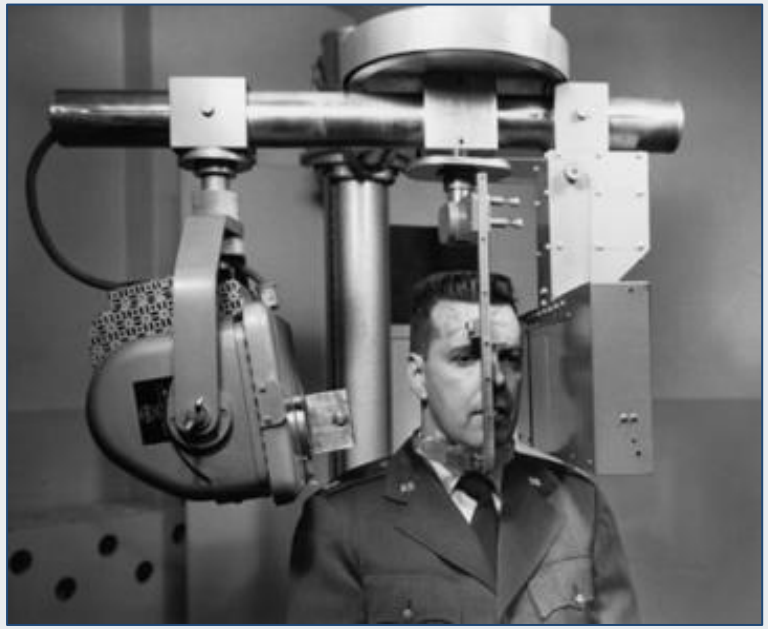
FIG. 27.—*The right way to use a fire extinguisher*

Source: NIST

NIST Background, cont.

NIST collaborated with the American Dental Association (ADA), which resulted in the invention of the panoramic X-ray machine.

- Collaboration began in WW1
- Partnership between NIST and the ADA
- January 1, 1953
- Led to the development of the panoramic X-ray
- Could image the entire mouth
- Minimized radiation/dental issues



Source: NIST

The First Digital Picture

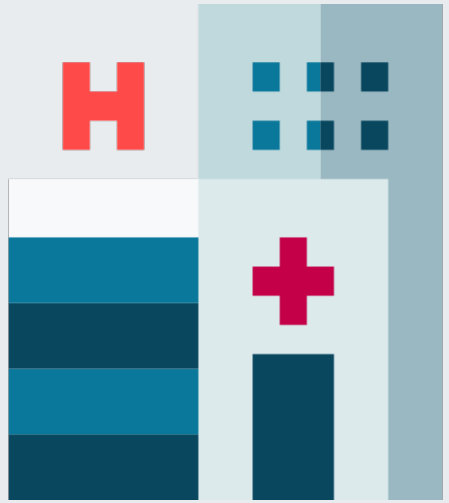
"Computer pioneer Russell Kirsch and his colleagues created the first digital image of his infant son Walden as part of their efforts to develop a way for the Standards Eastern Automatic Computer (SEAC), a first-generation computer designed and built at NIST, to recognize numbers and letters."

Source: NIST

NIST and Healthcare

In July 2022, NIST released an updated publication addressing how organizations can better protect personal health information in connection with the Cybersecurity Framework.

- NIST SP 800-66r2
- Aids compliance with the HIPAA Security Rule
- Helps protect personal health information
- Developed to better integrate with the Cybersecurity Framework
- Available as a resource guide for risk management



NIST and The National Cybersecurity Center of Excellence (NCCoE)

NIST collaborates with the NCCoE to help improve cybersecurity for the health sector through multiple projects and provides security guidance.

- Established in 2012
- Identifies cybersecurity challenges in healthcare
- Conducts projects to improve cybersecurity in healthcare
- Responses to emerging threats
  - COVID-19 and Telehealth
- Provides security guidance for technology
  - 5G, AI, IoT

Source: NIST

NIST Today – Cybersecurity

Mission: To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

- Helps businesses of all sizes understand, manage, and reduce cybersecurity risk
- Develops cybersecurity standards, guidelines, and best practices
- Addresses technological and future challenges

Source: sandboxaq

NIST and the Cybersecurity Framework

While it is non-regulatory, NIST has created several publications to assist organizations of all sizes with cybersecurity, including the well-known Cybersecurity Framework.

- Falls under the Department of Commerce
- Non-regulatory
- Has published comprehensive guidelines for cybersecurity
- Developed the Cybersecurity Framework
  - Has five core functions
  - Identify, Protect, Detect, Respond, and Recover
- These pillars represent a successful and holistic cyber program

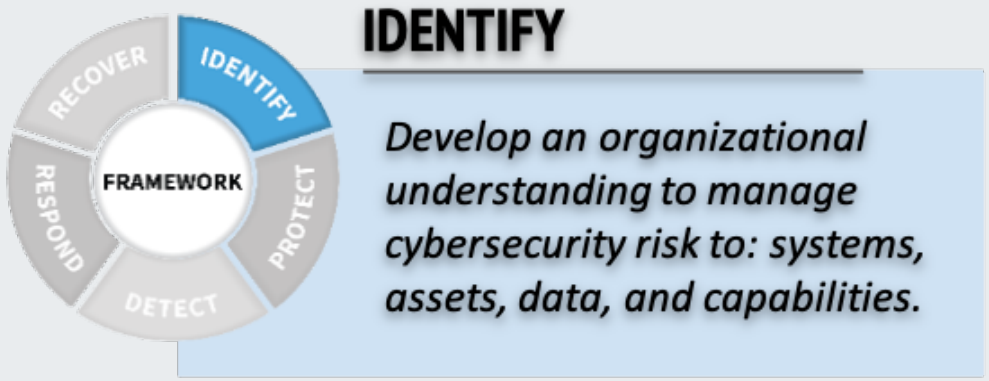
Source: kybersecure

The Cybersecurity Framework

Cybersecurity Framework - Identify

The Identify function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities.

- Develop understanding for organizations to manage cybersecurity risk to:
  - People, systems, assets, data, and capabilities
- The Identify Function is foundational for effective use of the framework
- Helps understand what supports critical functions
- Provides risk assessment opportunity
- Further understanding of roles and responsibilities
- Third-party risk assessments



Cybersecurity Framework - Protect

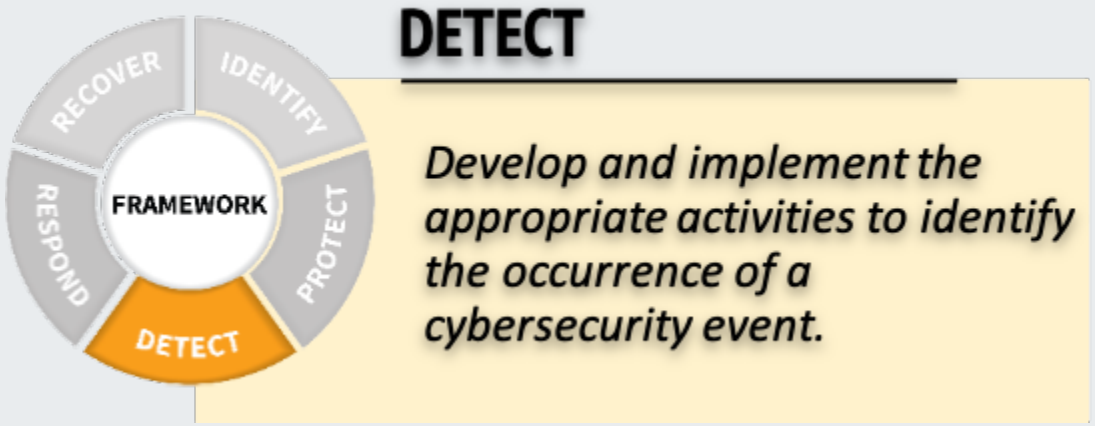
The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event.

- More proactive in nature
- Develop and implement safeguards
- Implementing control actions and training
- Establishes protective processes and procedures
- Supports limiting or containing a cyber event
- Maintenance
- Protective technology

Cybersecurity Framework - Detect

The Detect function emphasizes the importance of timely identification and response to cybersecurity incidents.

- Enables a timely discovery of cyber anomalies and events
- Security/continuous monitoring
- Detection processes
- Incident Response capabilities
- Enhance situational awareness
- Risk mitigation



Cybersecurity Framework - Respond

The Respond function deals with establishing an effective response plan in the event of a cybersecurity incident.

- Establishing effective planning
- Incident Response Plans
- Communication and coordination
- Incident analysis and mitigation
- Improving resilience
- Reporting and documentation

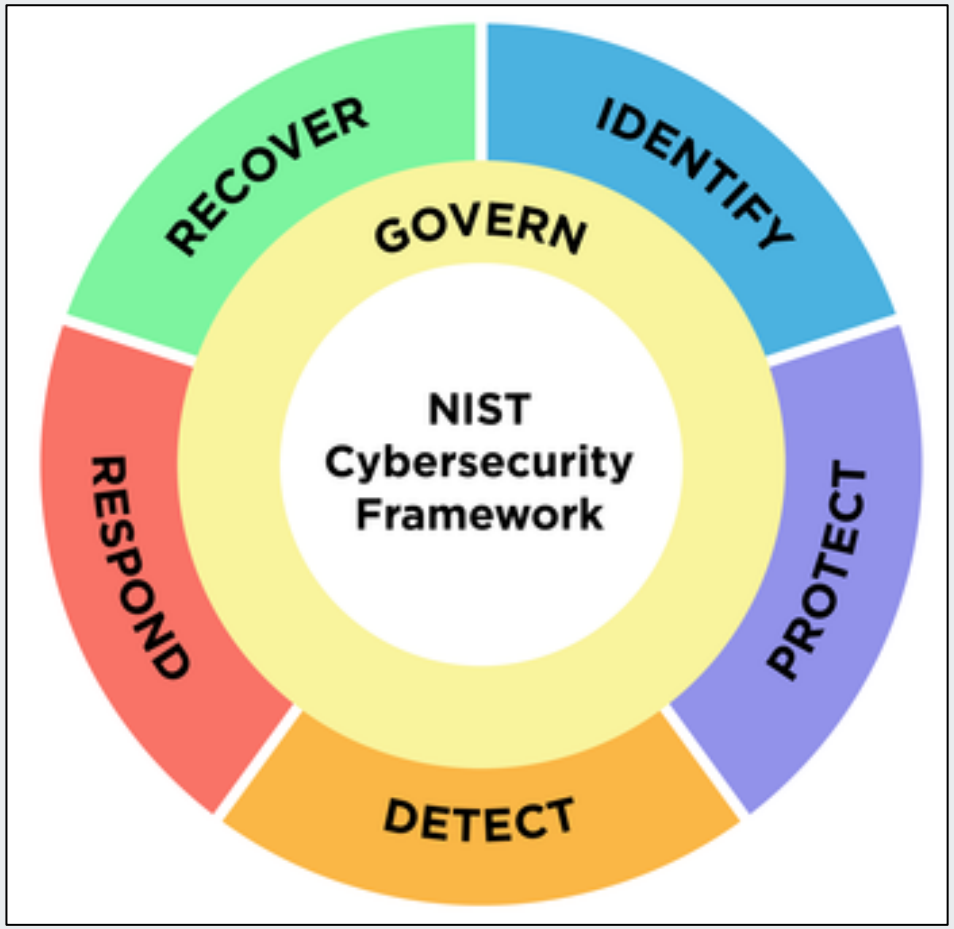
Cybersecurity Framework - Recover

The final step of the cybersecurity framework, Recover, emphasizes the importance of establishing a strategy for recovering from a cybersecurity incident.

- Planning for resilience
- Lessons learned
- Communication and coordination
- Continuous improvement
- Recovery planning
- Improving recovery capabilities

New NIST Framework

Currently in a draft phase, with an expected release date of early 2024.



Source: NIST

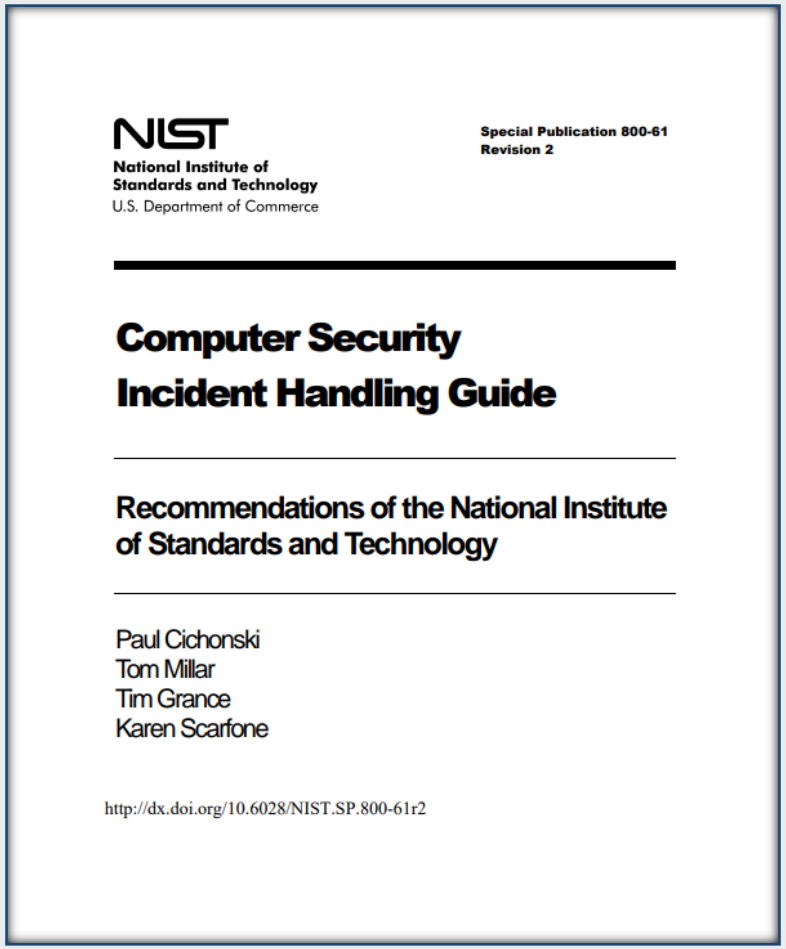
Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Cybersecurity Incident Response Plans

NIST Special Publication (SP) 800-61

- Computer Security Incident Handling Guide
  - NIST SP 800-61 r2
- Seeks to give organizations practical guidelines
- Not regulatory documents
- Primary focus: Detecting, analyzing, prioritizing, and handling incidents



What Is a Cybersecurity Incident Response Plan?

Create an Incident Response Policy

Prior to making an Incident Response Plan, it is recommended to create an incident response policy.

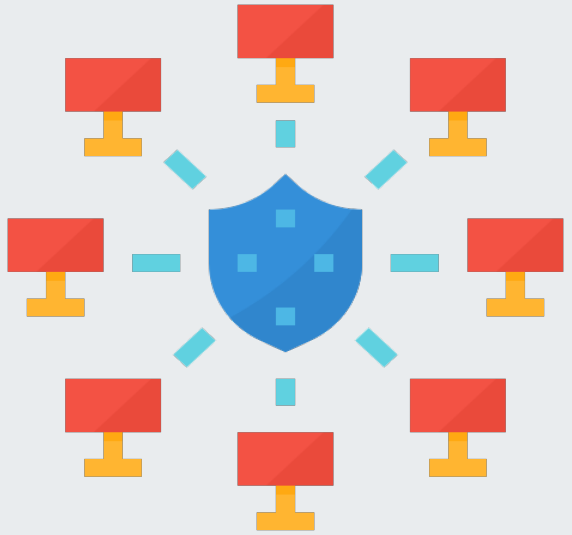
- Initially creating an Incident Response Policy:
  - Classify what a security incident is
  - Who is responsible for responding to an event?
  - Roles and responsibilities
  - Documentation
  - Reporting requirements

Source: pratum

Incident Response Plan Policy

According to NIST: “Policy governing incident response is highly individualized to the organization. However, most policies include the same key elements.”

- Provides a road map for a Statement of Management Commitment, which outlines the purpose and objectives of the policy incident response capabilities.
- Scope of the policy (to whom and what it applies, and under what circumstances)
- Definition of computer security incidents and related terms
- Organizational structure:
  - Definitions of roles and responsibilities
  - Levels of authority
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms



What Is a Cybersecurity Incident Response Plan?

- A written and systematic approach that establishes procedures and documentation.
- Incident Response Policy
- Can include items such as:
  - Guidelines
  - Roles and responsibilities
  - Communication plans
  - Standard protocols
- Incident Response Teams
- Tailored playbooks specific to the organization

Incident Response Plan Elements

An Incident Response Plan is a written document that helps your organization before, during, and after a security incident.

- Mission
- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- Incident response team communication
- Measuring the capability and effectiveness of incident response
- Planning for growth of incident response capabilities
- How the program fits into the overall organization

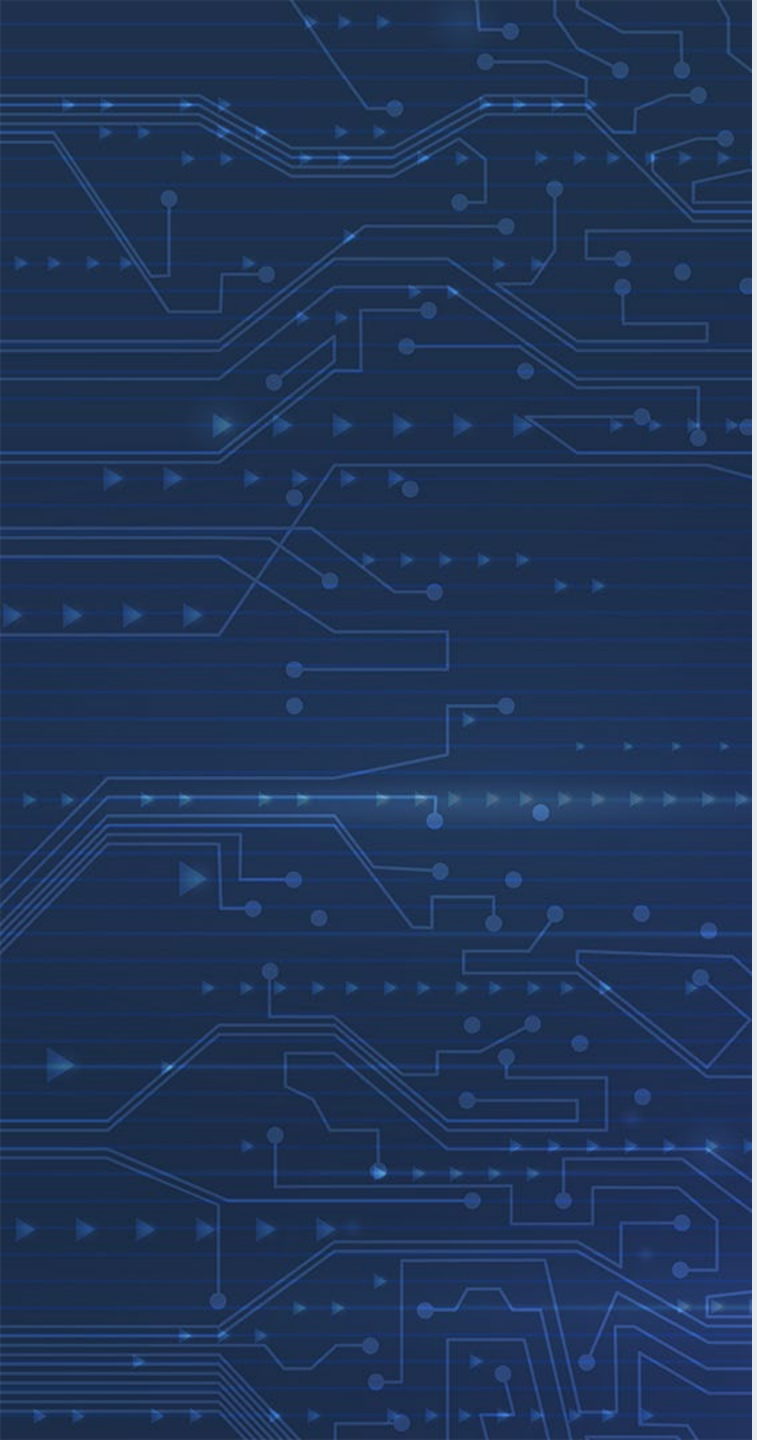
Incident Response Plans

NIST Special Publication (SP) 800-61 Revision 2 “Computer Security Incident Handling Guide” outlines the principles and steps for developing an Incident Response Plan.

- The NIST Incident Response Plan provides detailed guidelines for organizations.
- The objective is to minimize the overall impact of cyber incidents.
- Facilitate the recovery of operations
- The Incident Response Lifecycle – 4 Key Elements
  - Preparation and Planning; Detection and Analysis; Containment, Eradication, and Recovery; and Post-Incident Activities
  - Many incident response plans align with this lifecycle

Source: Swimlane

The Incident Response Lifecycle

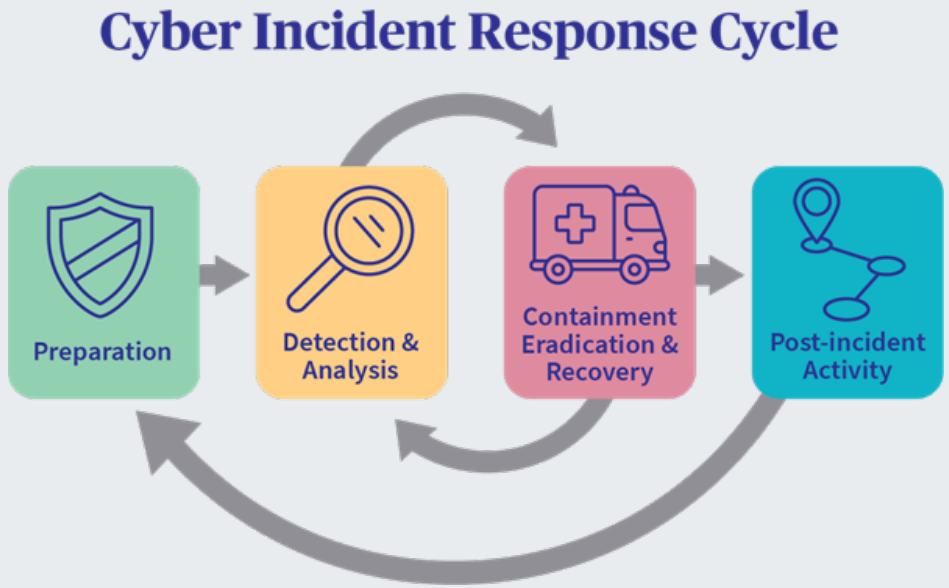


Preparation and Preventing Incidents

Preparation and Planning

The initial part of the lifecycle provides an opportunity for training, obtaining tools, and gathering resources while working towards preventing incidents through risk assessments.

- Identifying Assets and Risk:
  - Can include hardware, software, networks, and personnel
- Creating specialized response teams
- Identifying tools and resources needed
- NIST recommends classifying incidents into categories based on **severity** and **impact**.
- Organizations can tailor response strategies to be more effective.



Preparation and Planning: Tools and Resources

- Contact information
- On-call information
- Incident reporting mechanisms
- Issue tracking system
- Smartphones
- Encryption software
- War Room
- Secure storage facility
- Forensic workstations
- Laptops
- Spare workstations
- Blank removable media
- Portable printer
- Packet sniffers and protocol analyzers
- Digital forensic software
- Removeable media (Trusted)
- Evidence gathering accessories

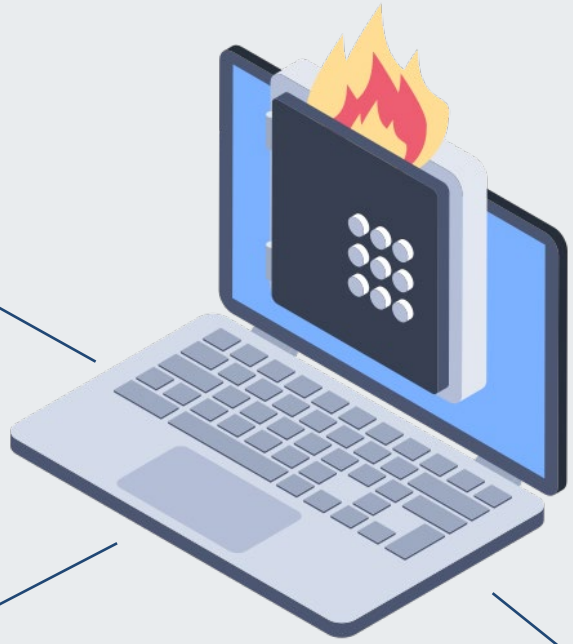
Jump Kits

Jump kits are portable, ready-to-go cases that contain the tools and resources a responder would need in the event of an incident.

- A portable case that carries items needed for an investigation.
  - Should always be ready to go
- Contains hardware, software, and other response items:
  - Cables, blank media, hard copies of documents
- Two laptops per incident handler is recommended:
  - One for malware analysis
  - One for actions that could infect the laptop

Source: ULINE

Preventing Incidents



Network Security

Malware Prevention

Patching Systems

Risk Assessments

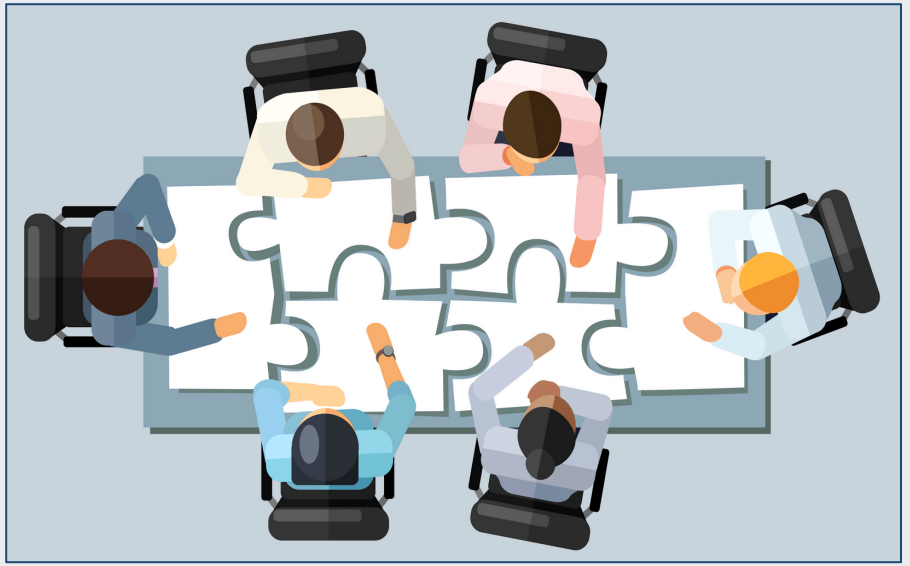
User Awareness and Training

Host Security

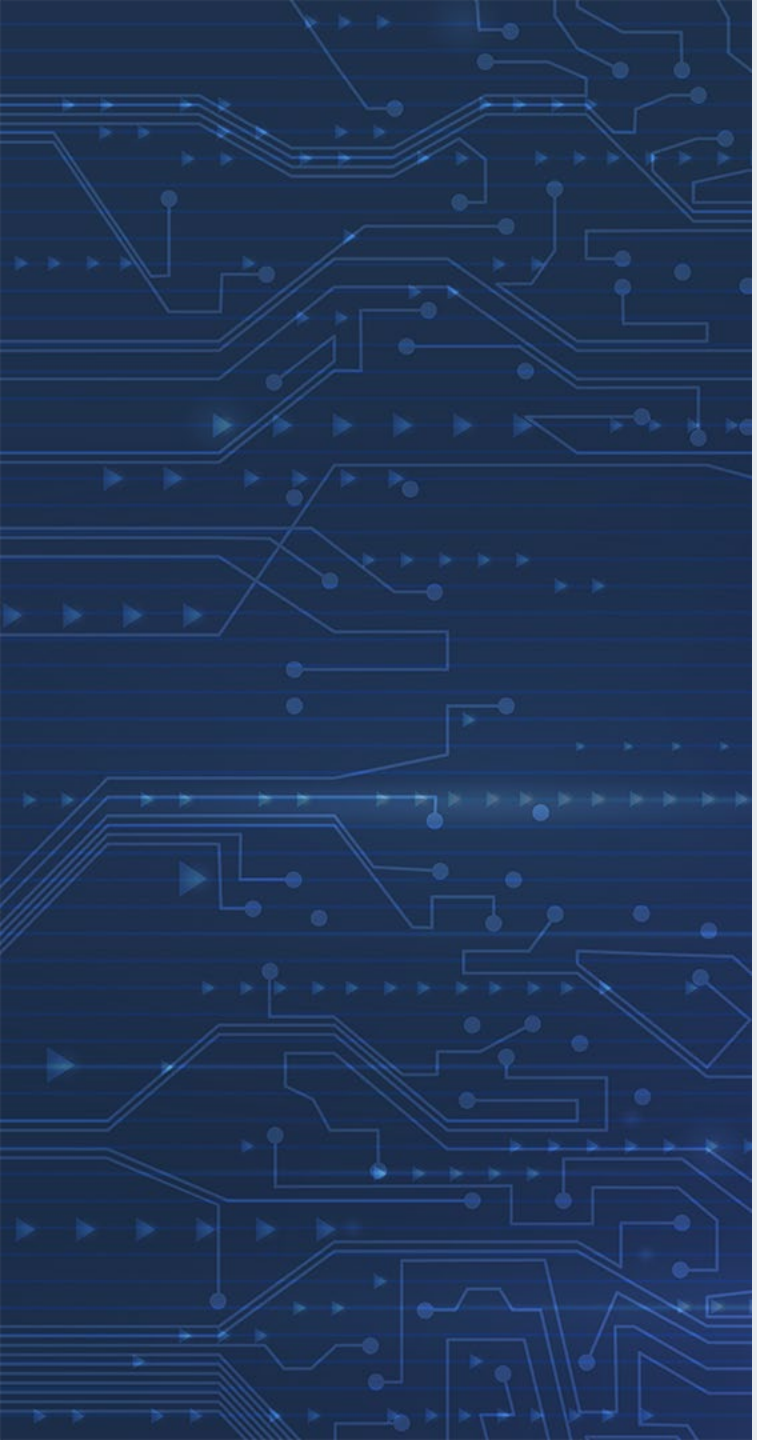
Training and Testing

Conducting training and testing for the response plan is a critical step, so that you can identify any weaknesses before a cyber incident occurs.

- After procedures and policies are established, test the plan before an incident takes place.
- Validates accuracy and usefulness
- Communication testing
- Ensuring functionality of tools
- Tabletop exercises
- Consider non-IT functions
  - Reverting to pen/paper
  - Diverting patients



Source: Intraprise Health



Detection and Analysis

Detection and Analysis

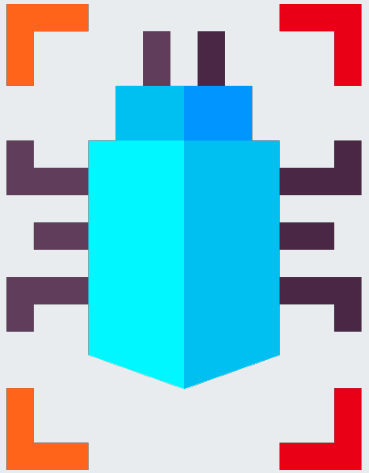
Incidents can occur in many ways, and it is not realistic to establish a response plan for every attack vector, since different incidents will require different response strategies. It is encouraged to develop procedures against some of the more common attack vectors.

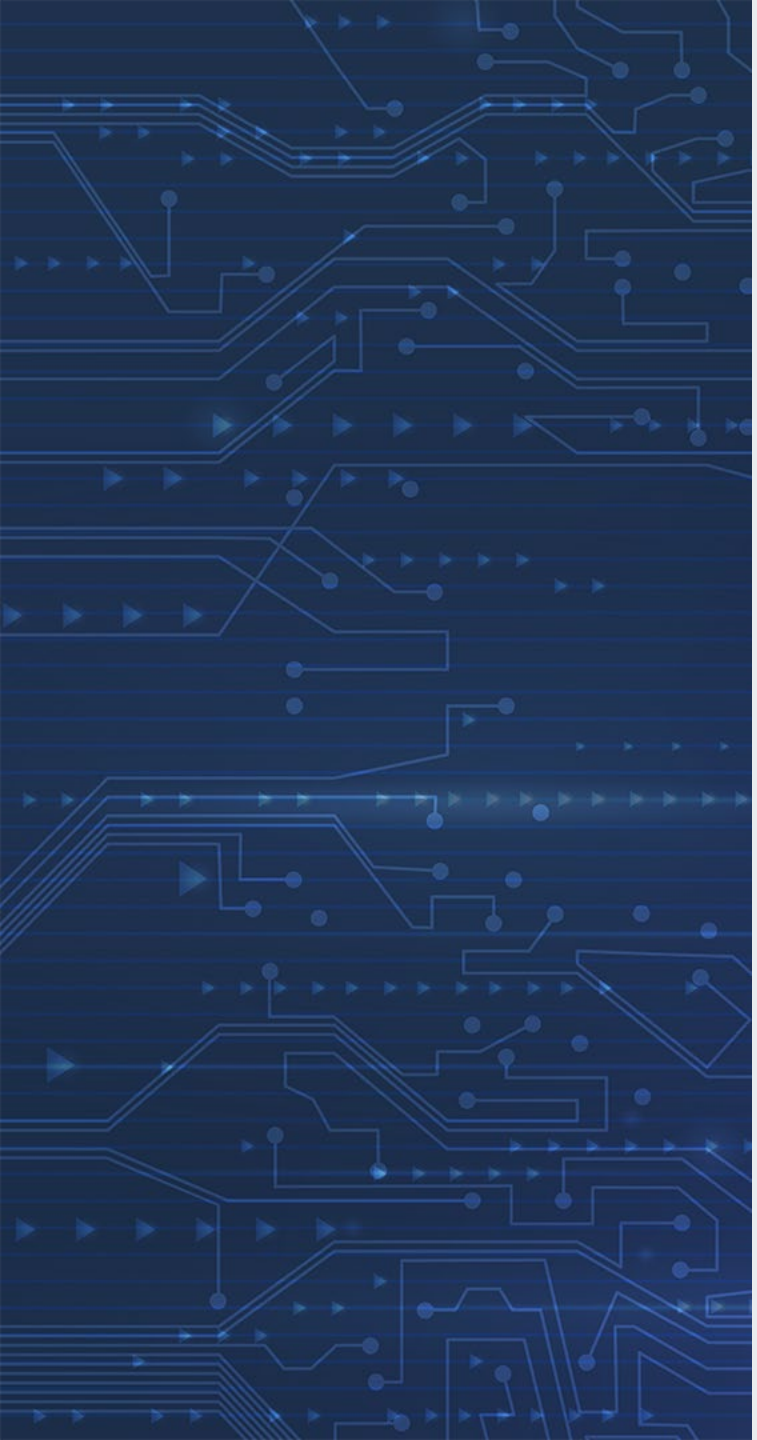
NIST Common Attack Vectors

- **External/Removable Media:** An attack executed from removable media or a device, such as a USB.
- **Attrition:** An attack that attempts to compromise, degrade, or destroy systems or services.
- **Web:** An attack executed from a website or a web-based application.
  - Cross-site scripting attack
  - Redirecting to another site
- **Email:** An attack executed through an email message or attachment (Phishing).

NIST Common Attack Vectors, cont.

- **Impersonation:** An attack that replaces something benign with something malicious.
  - Spoofing
  - Adversary-in-the-middle attacks
  - Rogue access points
- **Improper Usage:** Any incident resulting from a violation of an organization's acceptable usage policies.
- **Loss or Theft of Equipment:** The loss or theft of a computing device or media used by the organization.
- **Other:** Any other attack that does not fit into any of the above categories.





Containment, Eradication, and Recovery

Picking a Containment Strategy

Incident containment focuses on preventing the cyber incident from spreading and causing further damage.

- Potential damage and theft of resources
- Need for evidence preservation
- Service availability
- Time and resources needed to implement the strategy
- Effectiveness of the strategy
- Duration of the solution (workarounds and temporary solutions)

Containment, Eradication, and Recovery

Once a threat has been contained, incident response teams can work to eliminate the threat from the environment and prevent reoccurring attacks. Failure to do so can result in potential reinfection, or backdoors.

- Should be accomplished in a phased approach with recovery
  - Prioritize remediation steps

Eradication

- Deleting malware
- Disabling user accounts
- Mitigating vulnerabilities

Recovery

- Restoring systems
- Installing Patches
- Changing passwords

Containment, Eradication, and Recovery, cont.

While specific steps and recommended actions are not covered, there are still some encouraged best practices organizations can accomplish.

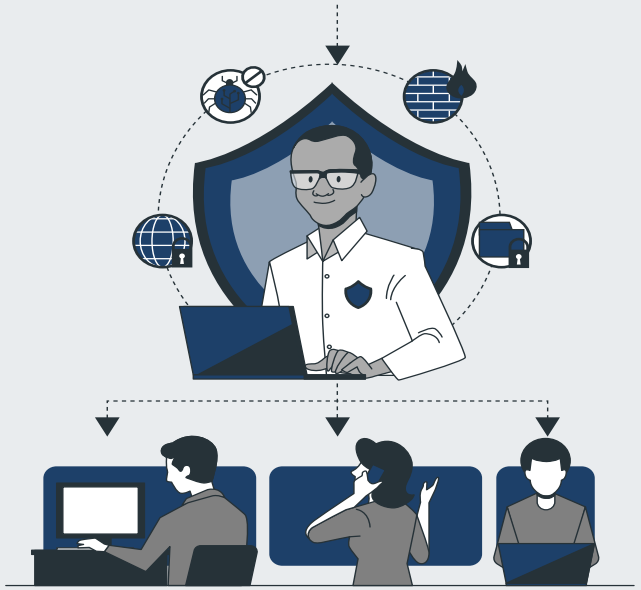
- **Timely response: A s**wift response is essential to contain and eradicate the threat.
- **Detailed Analysis:** Conducting a post-incident analysis to understand how the breach occurred.
- **Patch Management:** Keeping software and systems up to date helps prevent known vulnerabilities from being exploited.
- **Monitoring and Validation:** Monitoring the network after eradication to ensure the threat has been eliminated.

Post-Incident Activities

Post-Incident Activities

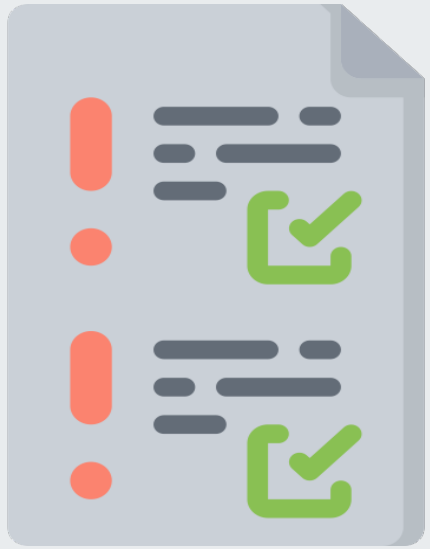
Post-incident activities are one of the most important parts of the incident response lifecycle, but unfortunately it is one of the most neglected.

- One of the most important parts of incident response
- Provides an opportunity to discuss threats, technology, and lessons learned
- Benefits improving security measures and handling processes
- Meetings can cover multiple incidents



Lessons Learned Example Questions

- What happened, at what time?
- How well was the staff performance?
- What information was needed sooner?
- Did any steps inhibit recovery?
- What would you do differently next time?
- Could information sharing be improved?
- Can corrective actions be implemented?
- Were additional tools or resources needed?



Incident Response Teams

Incident Response Teams

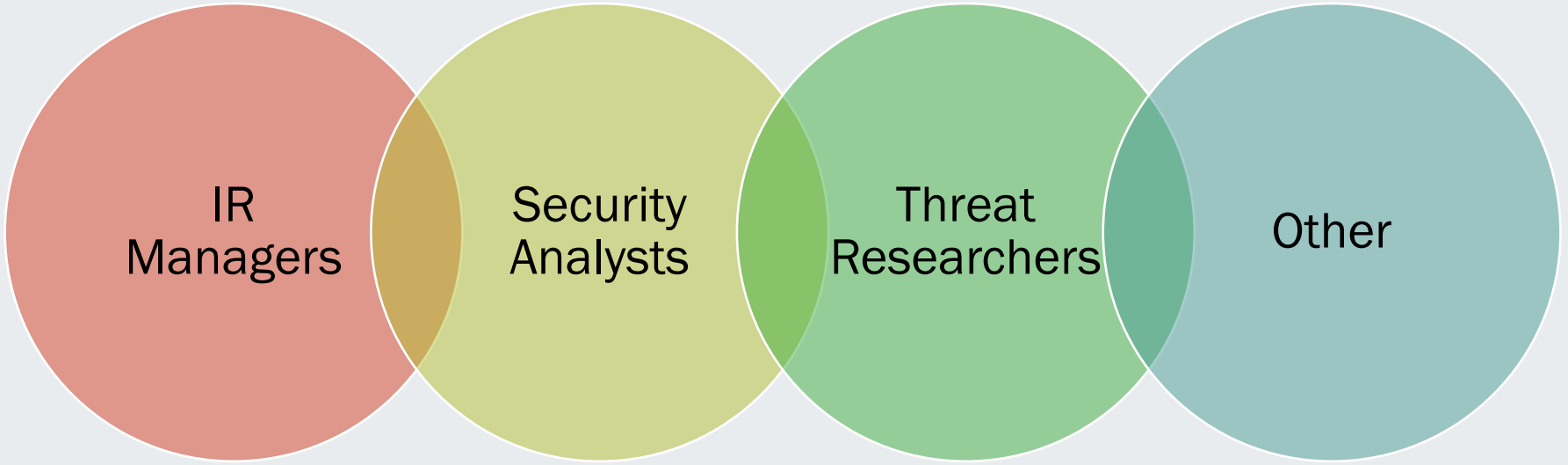
The type of organization should play a role in what type of team structure is assembled. Possible incident response team models are listed below:

Team Structure/Model	Type	Use
Central Incident Response Team	Single Response Team	Smaller organizations; minimal geographic diversity
Distributed Incident Response Team	Multiple Response Teams	Larger organizations; one team per segment/region
Coordinating Team	Provides advice to teams	Lacks authority

Staffing Models		
Employees	Partially Outsourced	Fully Outsourced

Team Role Considerations

There are several role considerations for a response team, and what fits best into the organization can vary by individual mission, but here are some common roles for an incident response team:



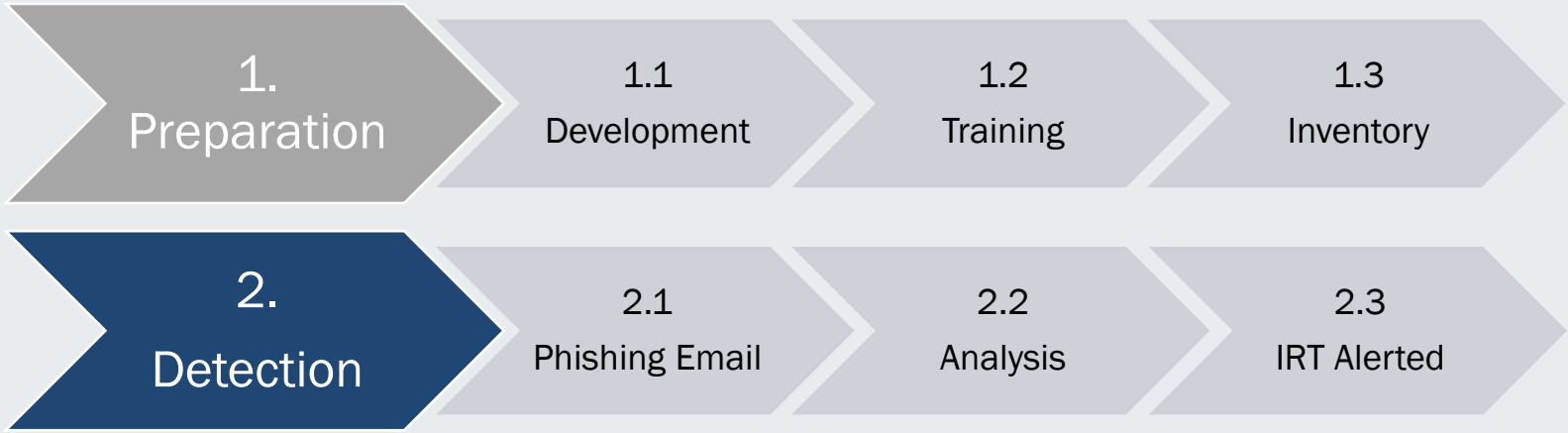
Incident Team Response Services

While the focus of an incident response team is on conducting incident response, there are additional services a team could offer:

Team Service	Benefit
Intrusion Detection	Analyze incidents quickly, enhance detection technologies.
Information Sharing	Collaborating partnerships, sharing groups, etc.
Education and Awareness	Enhanced reporting and detection
Advisory Distribution	Alerts on new threats/vulnerabilities

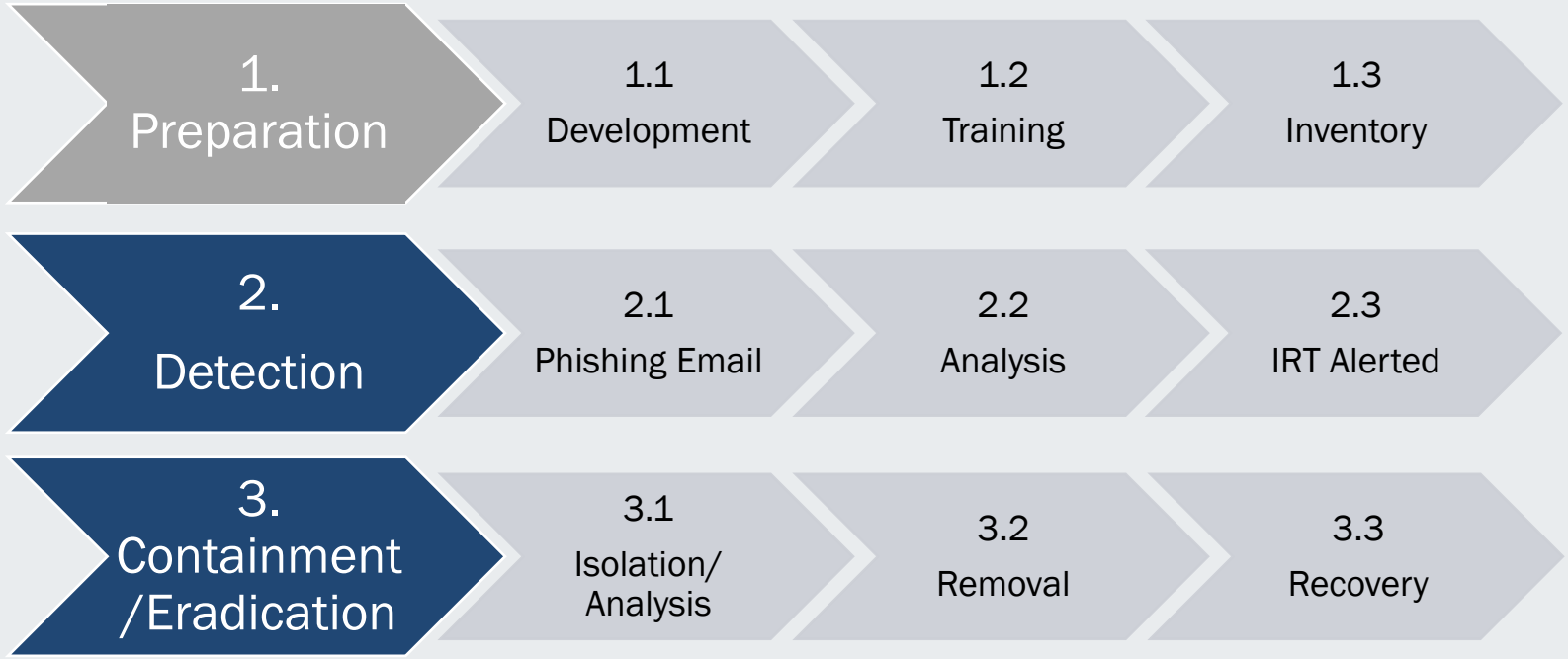
Scenario Walkthrough

Scenario: Detection



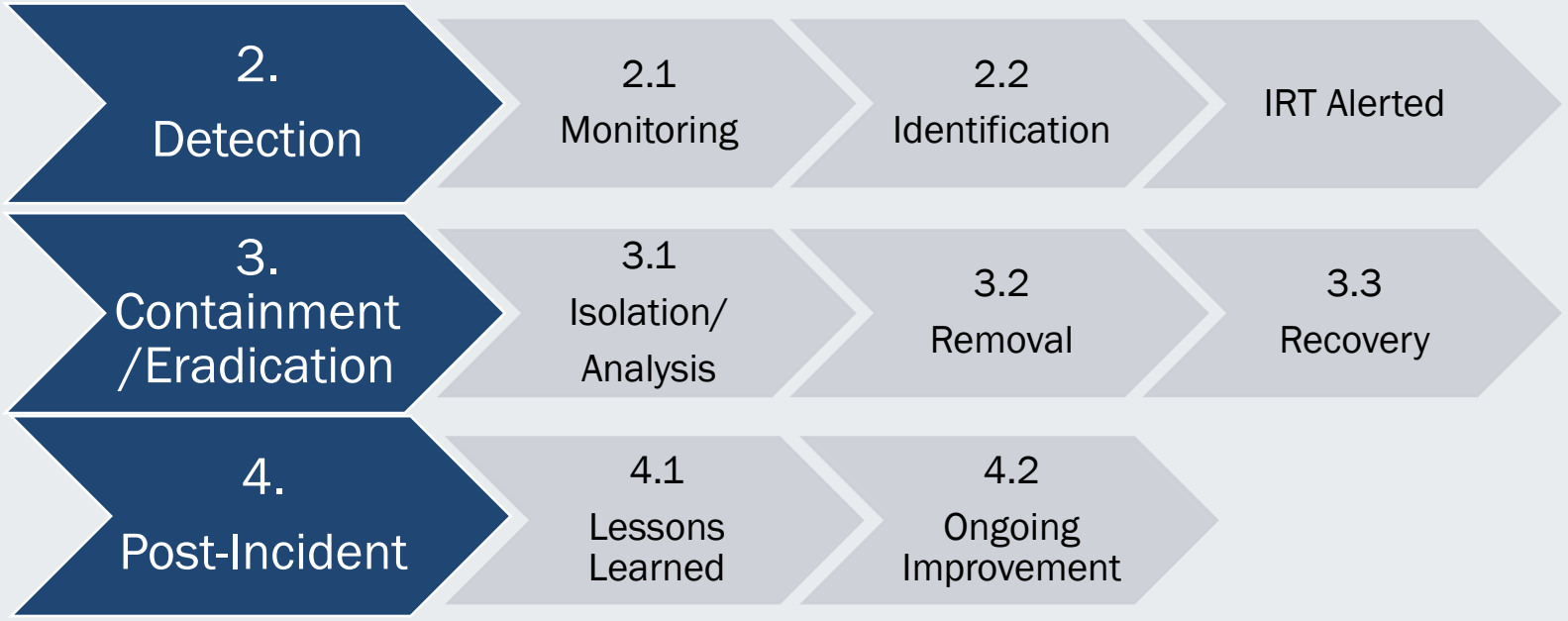
In this scenario, we will explore a cybersecurity incident where a phishing email leads to a ransomware attack against a hospital's network.

Scenario: Containment and Eradication



Analysis confirms the malicious nature of the email and identifies it as ransomware. The response team begins to work towards containing and eradicating the incident.

Scenario: Post-Incident Activities



After successfully removing the threat and the vulnerability, the team conducts post-incident activities to discuss what happened and what can be improved.

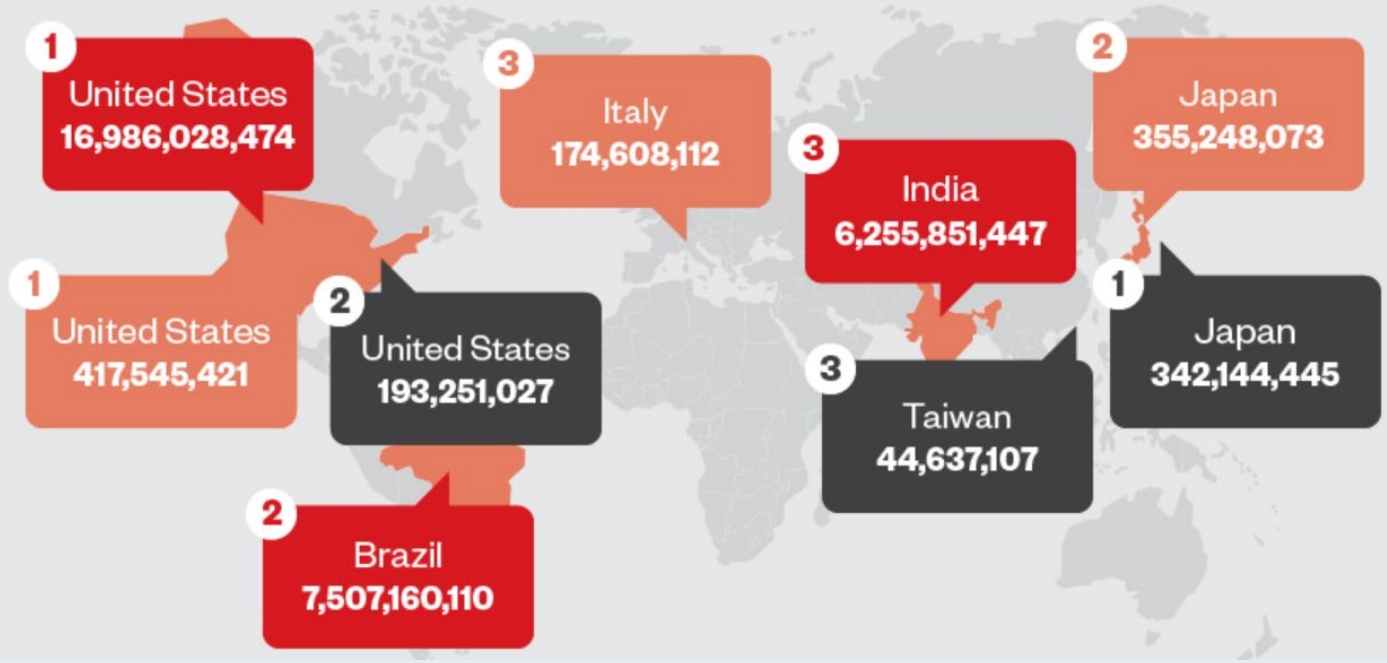
Why You Should Have an Incident Response Plan

TrendMicro 2023 Mid-Year Review

The United States is an active area for malicious targeting, and the HPH is one of the top five industries affected by malware campaigns.

Top 3 Countries

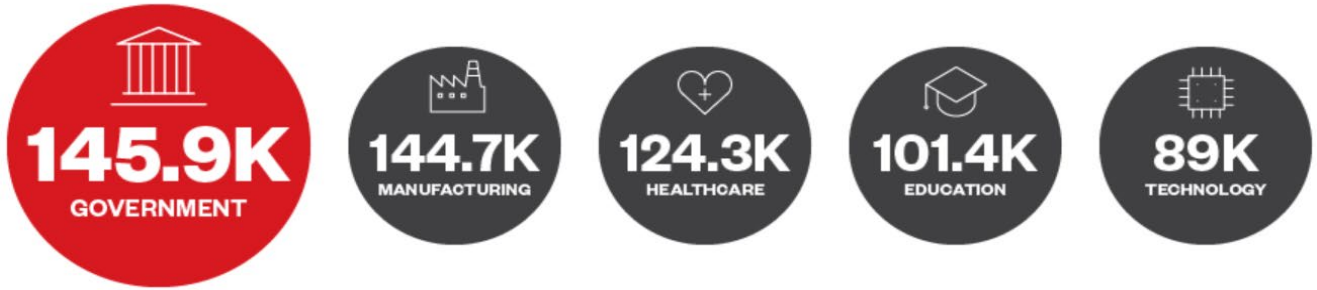
with risk events, malware detection, and malicious URL access



Top 5 Industries

affected by malware campaigns

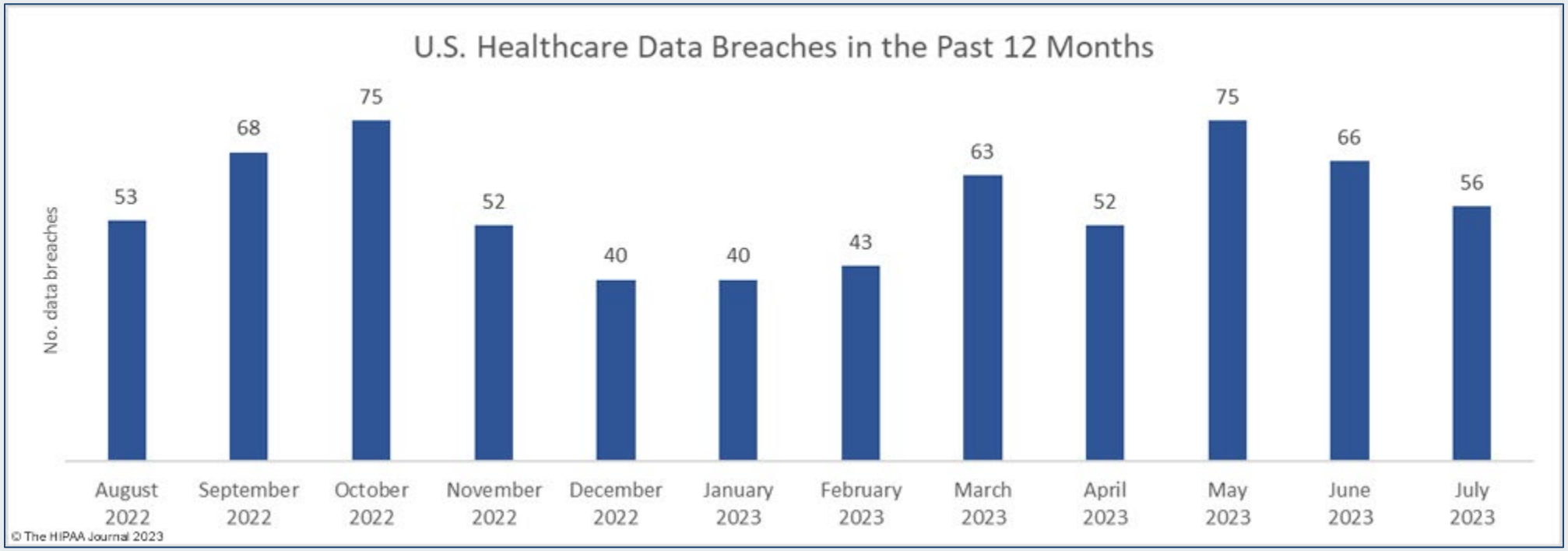
In the first half of 2023, malware campaigns targeted government organizations the most with 145,912 detections.



Source: TrendMicro

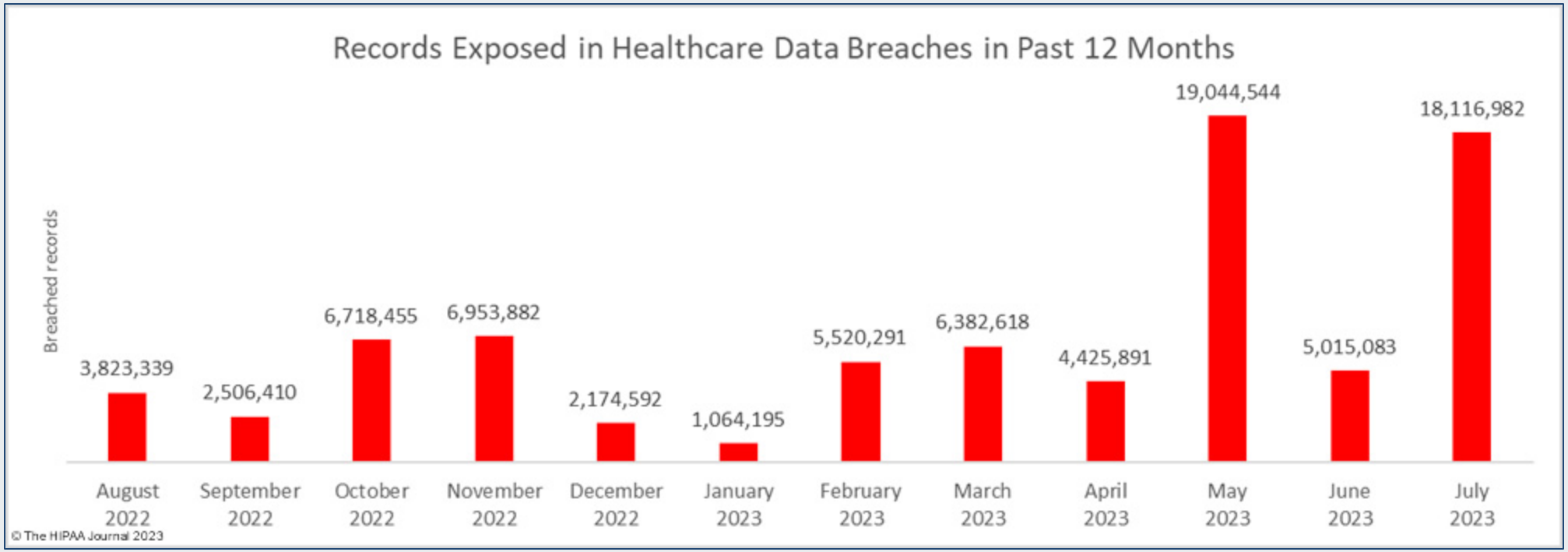
U.S. Healthcare Data Breaches, August 2022–July 2023

Data from the HIPAA Journal shows data breaches against healthcare from August 2022 to July 2023.



Source: HIPAA Journal

Data from the HIPAA Journal shows the number of records exposed in healthcare data breaches from August 2022 to July 2023.

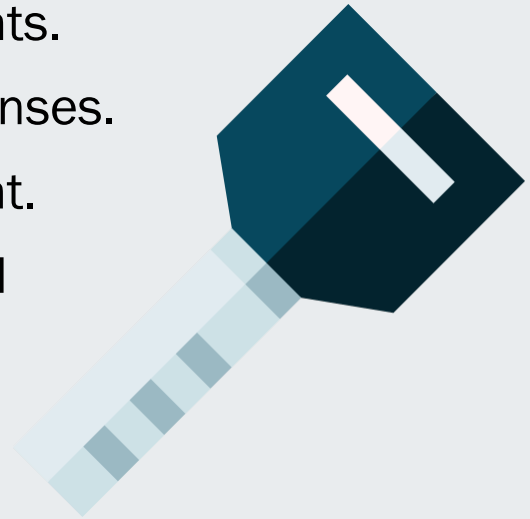


Source: HIPAA Journal

Incident Response Plans: Key Take-Aways

NIST Special Publication (SP) 800-61 Revision 2, “Computer Security Incident Handling Guide,” outlines the principles and steps for developing an Incident Response Plan.

- Incident Response Plans provide detailed guidelines for organizations.
- Organizations can follow and adopt widely-accepted best practices.
- Creates a standardized and common language for approaching incidents.
- NIST Incident Response Plans emphasize quick and coordinated responses.
- Engaging in post-incident analysis encourages continuous improvement.
- Creates opportunity to learn from mistakes, identify vulnerabilities, and enhance planning.



Resources

Incident Response Plan Resources

NIST Guidance:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST Contingency Planning:

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Coordinated Healthcare Incident Response Plan (CHIRP):

HIC-CHIRP-FINAL_1.pdf (healthsectorcouncil.org)

CISA Guidance:

https://www.cisa.gov/sites/default/files/2023-02/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks-508c.pdf

CISA Incident Response Plan Basics:

https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

ASPR HPH Cybersecurity Framework Implementation Guide:

Healthcare Sector Cybersecurity Framework Implementation Guide 1.1 (hhs.gov)

ASPR TRACIE (National Response Framework):

https://asprtracie.hhs.gov/technical-resources/resource/1746/national-response-framework

ASPR Incident Response Framework:

HHS/ASPR Incident Response Framework v2.1 (phe.gov)

National Cyber Incident Response Plan:

https://www.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

Reference Materials

References

- Cichonski, Paul. Millar, Tom. Grance, Tim. Scarfone, Karen. Computer Security Incident Handling Guide. NIST. Computer Security Incident Handling Guide (nist.gov)
- From NBS to NIST. NIST. https://www.nist.gov/pao/nist-100-foundations-progress/nbs-nist
- Panoramic X-Ray Machine. NIST. https://www.nist.gov/timeline#event-774311
- The First Digital Image. NIST. https://www.nist.gov/timeline#event-774341
- NIST. NIST Updates Guidance for Health Care Cybersecurity. July 21, 2022. NIST Updates Guidance for Health Care Cybersecurity | NIST
- NIST. NCCoE. Working Together for Cybersecurity. Homepage | NCCoE (nist.gov)
- "NIST Incident Response". Cynet. https://www.cynet.com/incident-response/nist-incident-response/#:~:text=The%20NIST%20incident%20response%20process%20is%20a%20cyclical%20activity%20featuring,containment%2Feradication%2C%20and%20recovery.

- Hall, Ben. LaBello, Sammi. Creating an Incident Response Plan. Pratum. March 10, 2020. Creating an Incident Response Plan - Pratum
- Duran, Dan. NIST Incident Response Plan: Steps and Template. Linkedin. July 7, 2022. https://www.linkedin.com/pulse/nist-incident-response-plan-steps-template-dan-duran
- Welekwe, Amakiri. “How to Create a Cyber Security Incident Response Plan for Your Organization”. Comparitech. April 26, 2023. https://www.comparitech.com/net-admin/create-cyber-security-incident-response-plan/
- NIST. Cybersecurity Framework Quick Start Guide. https://www.nist.gov/cyberframework/getting-started/quick-start-guide
- Bresnahan, Ethan. NIST Cybersecurity Framework Core Explained. https://www.cybersaint.io/blog/nist-cybersecurity-framework-core-explained#:~:text=NIST%20CSF%3A%20Protect&text=The%20Protect%20function%20of%20the,of%20a%20potential%20cybersecurity%20event.

- NIST. The Five Functions. https://www.nist.gov/cyberframework/online-learning/five-functions
- Bykowski, Katie. The Role of Preparation and Process in Incident Response. Swimlane. June 12, 2020. https://swimlane.com/blog/the-role-of-preparation-and-process-in-incident-response/
- CISA. Healthcare and Public Health Sector. https://www.cisa.gov/stopransomware/healthcare-and-public-health-sector
- CISA. Incident Response Plan (IRP) Basics. https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf
- Anderson, Erin. How to Comply in 2020 With The 5 Functions of The NIST Cybersecurity Framework. Forescout. January 9, 2020. https://www.forescout.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework/
- Intraprise Health. Tabletop Exercises in Cybersecurity: Unappreciated and Underutilized. July 28, 2023. https://intraprisehealth.com/tabletop-exercises-unappreciated-and-underutilized/

- TrendMicro 2023 Midyear Cybersecurity Threat Report https://documents.trendmicro.com/images/TEx/articles/Risk_Landscape_infographic-aypd962.png
- Cynet. NIST Incident Response. https://www.cynet.com/incident-response/nist-incident-response/#key-roles-in-an-incident-response-team
- A Guide to the NIST Cybersecurity Framework. DarkReading. September 30, 2020. https://www.darkreading.com/physical-security/a-guide-to-the-nist-cybersecurity-framework
- Kybersecure. 3 Reasons to Align With the NIST Cybersecurity Framework. April 19, 2019. https://kybersecure.com/3-reasons-to-align-with-nist-cybersecurity-framework/

Questions

FAQ

Upcoming Briefing

- November 16 – Emotet Malware: The Enduring and Persistent Threat to the Health Sector

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings

Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

HC3 and Partner Resources

Health Sector Cybersecurity Coordination Center (HC3)

- HC3 Products

405(D) Program and Task Group

- 405(D) Resources
- 405(D) Health Industry Cybersecurity Practices

Food and Drug Administration (FDA)

- FDA Cybersecurity

Cybersecurity and Infrastructure Security Agency (CISA)

- CISA Stop Ransomware
- CISA Free Cybersecurity Tools
- CISA Current Activity
- CISA Incident Reporting

Federal Bureau of Investigation (FBI)

- FBI Cybercrime
- FBI Internet Crime Complaint Center (IC3)
- FBI Ransomware

Health Sector Coordinating Council (HSCC)

- HSCC Recommended Cybersecurity Practices
- HSCC Resources

Health – Information Sharing and Analysis Center (H-ISAC)

- H-ISAC Threat Intelligence: H-ISAC Hacking Healthcare
- H-ISAC White Papers

CPE Credits

This 1-hour presentation by HHS HC3 provides you with 1 hour of CPE credits based on your Certification needs.

The areas that qualify for CPE credits are Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Typically, you will earn 1 CPE credit per 1 hour time spent in an activity. You can report CPE credits in 0.25, 0.50 and 0.75 increments.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

WWW.HHS.GOV/HC3

HC3@HHS.GOV