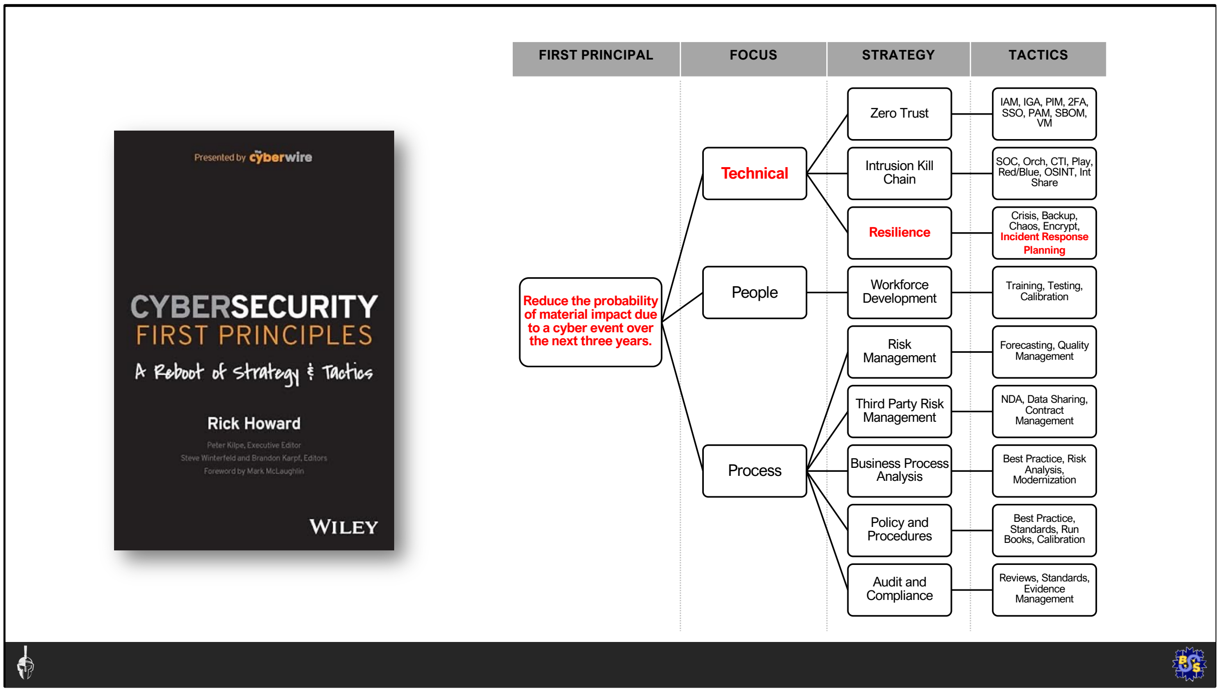
Incident Response Planning Introduction

BSIDES BLOOMINGTOM 2024



Presented by cyberwire

CYBERSECURITY FIRST PRINCIPLES

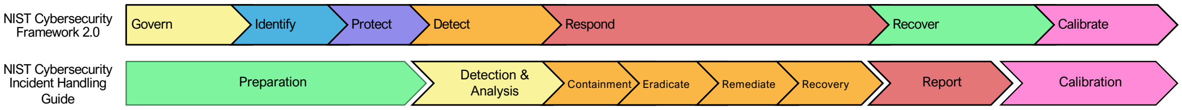
A Reboot of Strategy & Tactics

Rick Howard

Peter Kilpe, Executive Editor
Steve Winterfeld and Brandon Karpf, Editors
Foreword by Mark McLaughlin

WILEY

FIRST PRINCIPAL	FOCUS	STRATEGY	TACTICS
Reduce the probability of material impact due to a cyber event over the next three years.	Technical	Zero Trust	IAM, IGA, PIM, 2FA, SSO, PAM, SBOM, VM
		Intrusion Kill Chain	SOC, Orch, CTI, Play, Red/Blue, OSINT, Int Share
		Resilience	Crisis, Backup, Chaos, Encrypt, Incident Response Planning
	People	Workforce Development	Training, Testing, Calibration
	Process	Risk Management	Forecasting, Quality Management
		Third Party Risk Management	NDA, Data Sharing, Contract Management
		Business Process Analysis	Best Practice, Risk Analysis, Modernization
		Policy and Procedures	Best Practice, Standards, Run Books, Calibration
		Audit and Compliance	Reviews, Standards, Evidence Management

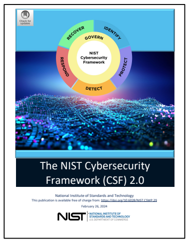


NIST Cybersecurity Framework 2.0

Govern → Identify → Protect → Detect → Respond → Recover → Calibrate

NIST Cybersecurity Incident Handling Guide

Preparation → Detection & Analysis → Containment → Eradicate → Remediate → Recovery → Report → Calibration



Check for updates

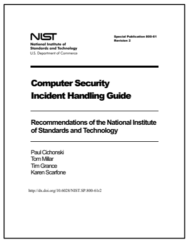
The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29

February 26, 2024

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf



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

Special Publication 800-61
Revision 2

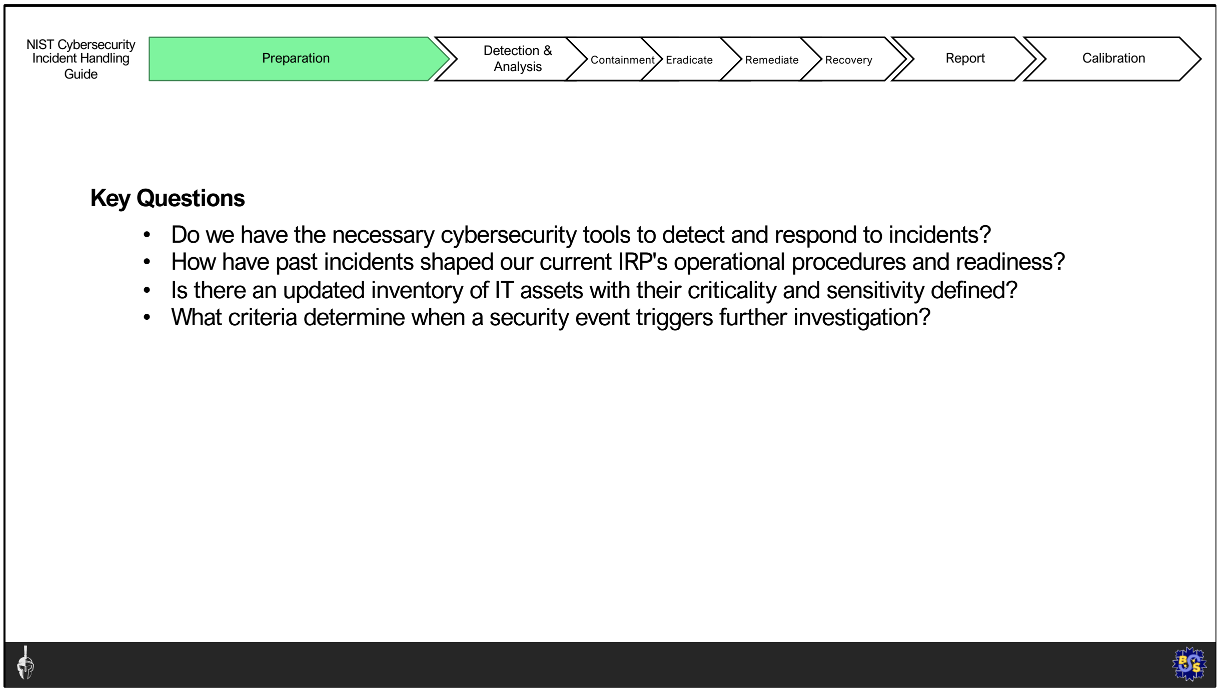
Computer Security Incident Handling Guide

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

NIST SP800-61 r2 Computer Security Incident Handling Guide
https://csrc.nist.gov/pubs/sp/800/61/r2/final



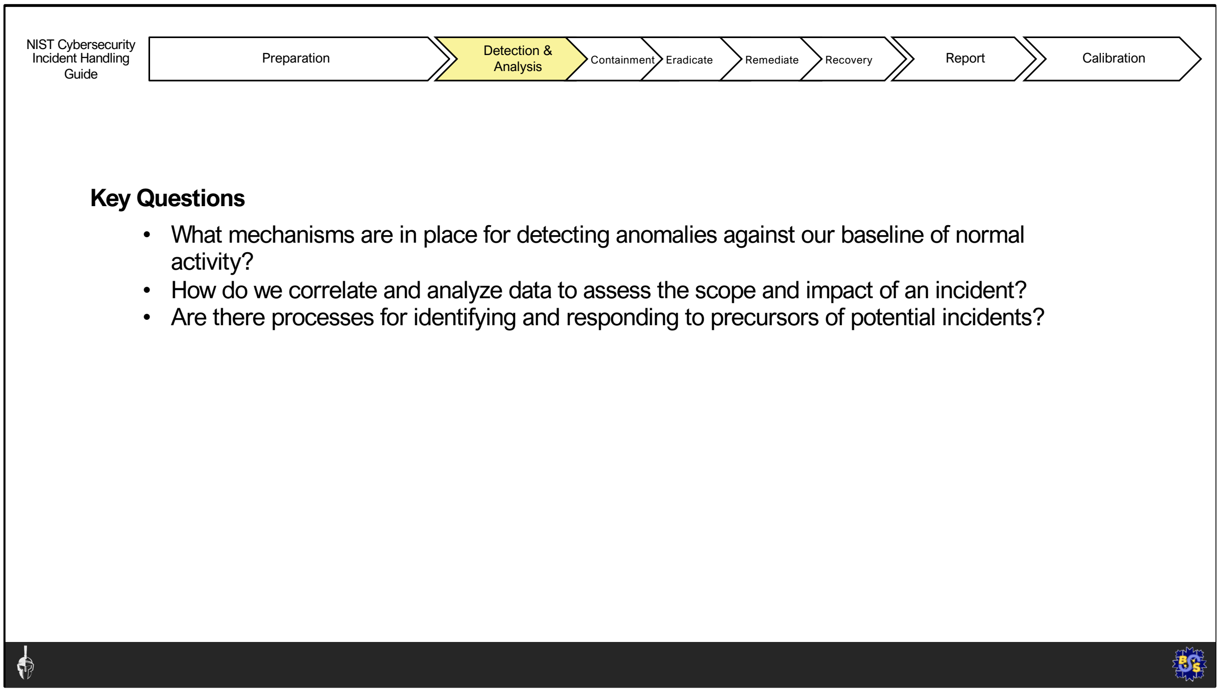
NIST Cybersecurity Incident Handling Guide

Preparation → Detection & Analysis → Containment → Eradicate → Remediate → Recovery → Report → Calibration

Key Questions

- Do we have the necessary cybersecurity tools to detect and respond to incidents?
- How have past incidents shaped our current IRP's operational procedures and readiness?
- Is there an updated inventory of IT assets with their criticality and sensitivity defined?
- What criteria determine when a security event triggers further investigation?

Preparation
Technical responders should ensure that they have both the cybersecurity investments to detect and respond to incidents when they occur. This preparation includes making appropriate investments in these capabilities and to those that will be used throughout the process. A full IRP would detail these capabilities and help develop the operational procedures necessary to execute the IRP. Your role is to ensure that the EIRP preparation phase registers the risks appropriate to your organization and makes the necessary investments here to ensure the IRP can execute efficiently and effectively. The effectiveness of past incidents or lessons learned from a technical IRP tabletop can be instrumental in understanding your readiness.
• Compiling an inventory of IT assets, their importance, and sensitivity. (asset management - inventory)
• Establishing a baseline of normal activity for monitoring purposes. (behavioral analysis)
• Determining which security events warrant further investigation. (risk management - sensitivity analysis)
• Creating detailed response steps for common types of incidents. (policy & procedure - playbooks)



NIST Cybersecurity Incident Handling Guide

Preparation | Detection & Analysis | Containment | Eradicate | Remediate | Recovery | Report | Calibration

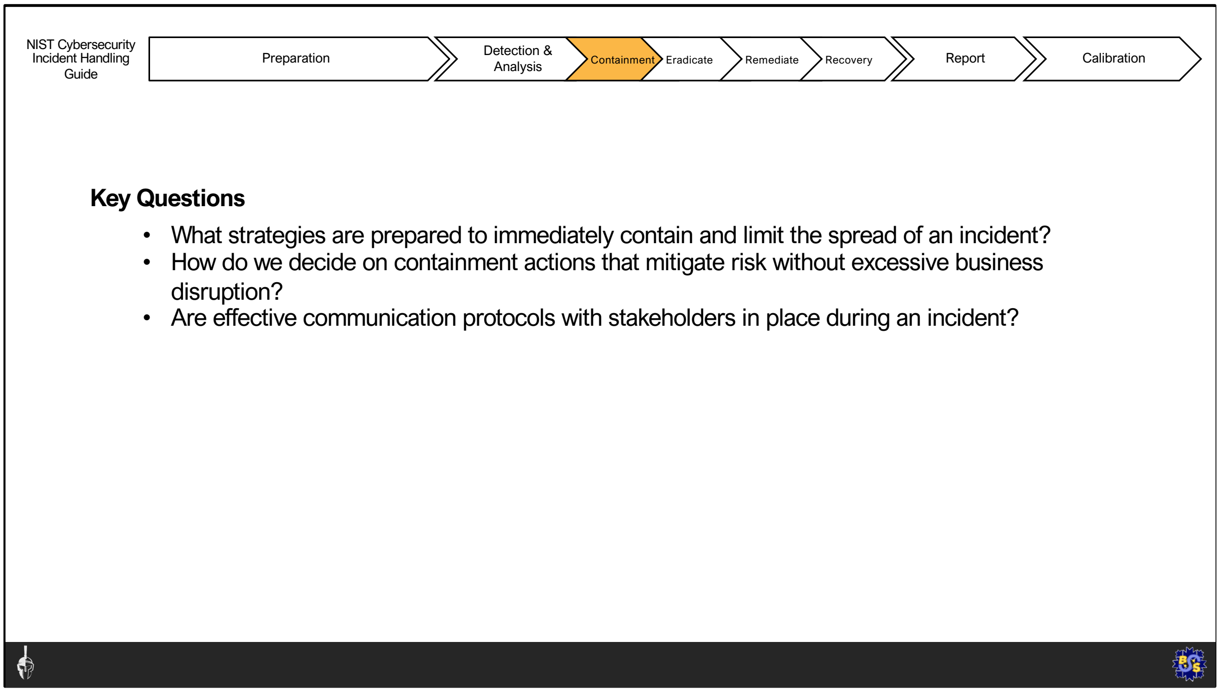
Key Questions

- What mechanisms are in place for detecting anomalies against our baseline of normal activity?
- How do we correlate and analyze data to assess the scope and impact of an incident?
- Are there processes for identifying and responding to precursors of potential incidents?

Detection & Analysis
Technical responders need to be able to detect and analyze threats as they occur in the environment. During the preparation phase, as these risks are identified, the technical aspect of this is to ensure that there are means to understand the technical landscape. For incidents, usually this means monitoring potential threat vectors, like your email system, internet connection, applications that may be vulnerable, or loss of assets like a stolen computer. Your technical team during this phase should be constantly looking for signs that an incident has occurred. Once this does happen, and it will if they are able to execute this phase correctly, your responsibility will be to participate in a risk determination step within the EIRP. The effectiveness of this step is based on the ability to correctly identify the incident and the impact to the organization because this will help calibrate your team's response to the evolving incident.

- *Gathering data from IT systems, security tools, public information, and organizational insights to identify potential and actual indicators of incidents.*
- *Analyzing data against the established baseline to identify deviations that may indicate a security incident.*
- *Correlating related events to assess the scope and impact of the incident.*

- *Identifying precursors to prevent potential future incidents.*



NIST Cybersecurity Incident Handling Guide

Preparation › Detection & Analysis › Containment › Eradicate › Remediate › Recovery › Report › Calibration

Key Questions

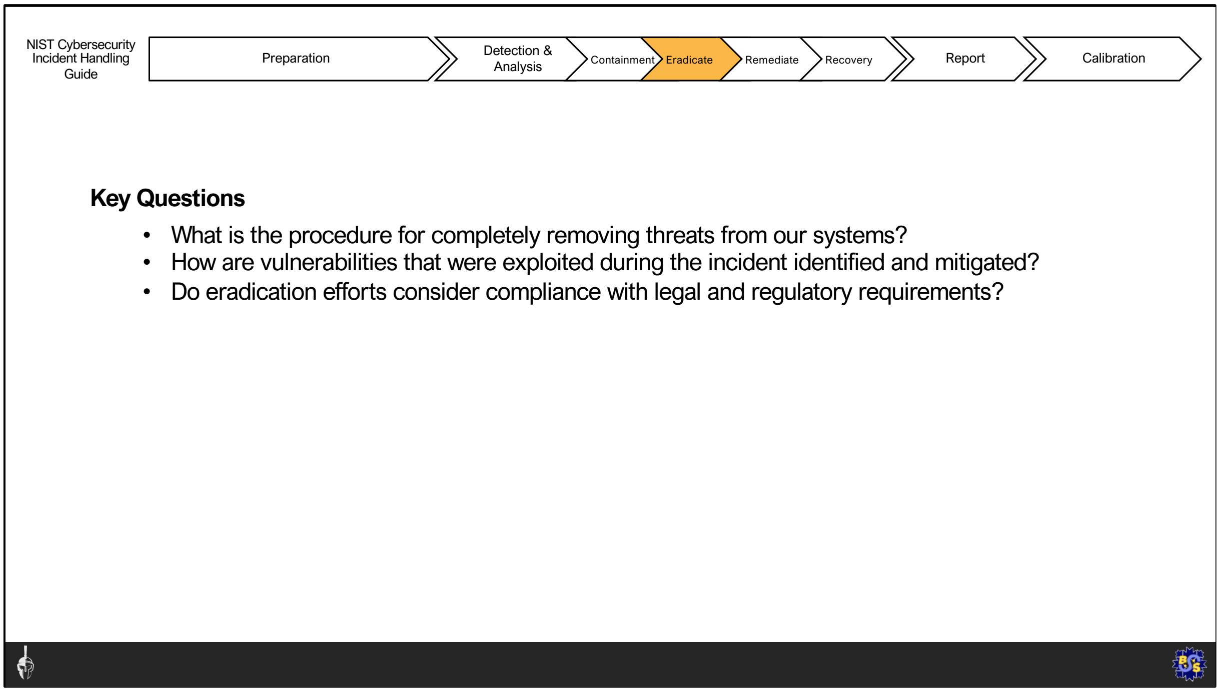
- What strategies are prepared to immediately contain and limit the spread of an incident?
- How do we decide on containment actions that mitigate risk without excessive business disruption?
- Are effective communication protocols with stakeholders in place during an incident?

Containment
Containment is just what it sounds like. The singular goal in this phase is to stop losses and contain the damage. Largely, the success of this phase depends on two factors. First is the ability of the technical team to have correctly detected and analyzed the incident as it is then known, and second is to make appropriate decisions at your level to determine the risk to the organization and measure the response of the team to limit damage while not inflicting unnecessary pain from the containment activity. For example, if your organization is experiencing a malware infection, you could make the risk determination that it is better to disconnect critical systems from the network than allow the malware to spread; however, this action will make that critical system unavailable to users while preserving its state.

Therefore, Risk Determination is a critical step in your executive incident response capability that must precede the technical act of containment. Once these key steps are completed, the containment step will develop a containment strategy which will govern the process for implementing a technical means for acting on your risk determination. Remember that you may be asked to revisit this step if later in the incident it is determined that the *initial scope of the incident has changed.*

- *Implementing strategies to limit the spread of an incident and prevent further damage.*

- *Deciding on the containment strategy based on the potential impact of the incident.*
- *Ensuring that containment measures are effective without causing unnecessary disruption to business operations.*
- *Maintaining communication with relevant stakeholders to manage the situation.*



NIST Cybersecurity Incident Handling Guide

Preparation › Detection & Analysis › Containment › Eradicate › Remediate › Recovery › Report › Calibration

Key Questions

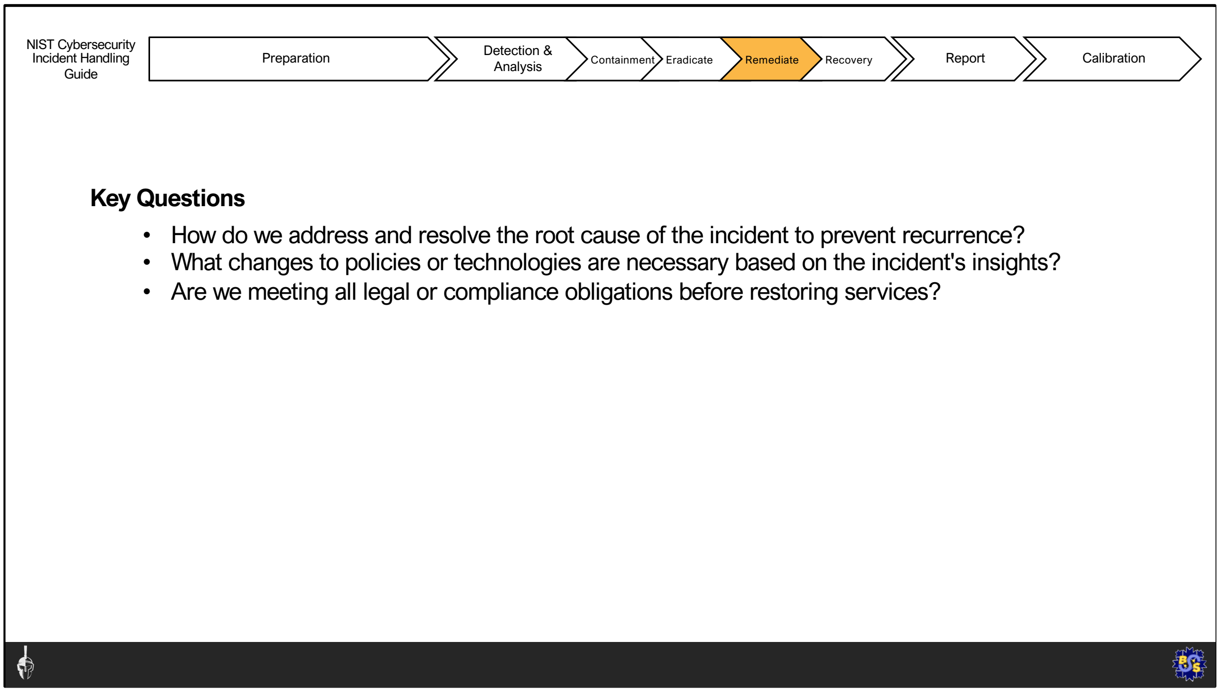
- What is the procedure for completely removing threats from our systems?
- How are vulnerabilities that were exploited during the incident identified and mitigated?
- Do eradication efforts consider compliance with legal and regulatory requirements?

Eradication

In the eradication phase, the technical team should have been able to appropriately contain the risk and is now considering how to remove it. While a large part of this technical step is just that, it will also create a eradication strategy that will be important to you in the remediation phase. For this reason, the EIRP will take this eradication strategy recommendation and begin to consider how this will inform your decision on remediation. You may decide for example that it is better to act conservatively and take steps to decommission or destroy assets in order to get core services back online. This may affect your ability to retain evidence or perform further forensic analysis that could be useful in the root cause analysis that the team will want to perform to ensure that you are safe from this attack in the future. The business decisions about how quickly you respond to a business and technology informed risk will drive the success of your company in being able to respond to this and future events. You should also consider during this phase whether as to if you have legal or compliance requirements that may require additional steps outside of the purview of the technical response team. This may include breach notification, legal requirements or other compliance considerations.

• Removing the components of the incident, such as malware or unauthorized access, from the affected systems.

• Identifying and mitigating all vulnerabilities that were exploited during the incident.
• Revisiting and improving security measures to prevent similar incidents.
• Preparing for the recovery process by ensuring that all traces of the incident have been removed.



NIST Cybersecurity Incident Handling Guide

Preparation → Detection & Analysis → Containment → Eradicate → Remediate → Recovery → Report → Calibration

Key Questions

- How do we address and resolve the root cause of the incident to prevent recurrence?
- What changes to policies or technologies are necessary based on the incident's insights?
- Are we meeting all legal or compliance obligations before restoring services?

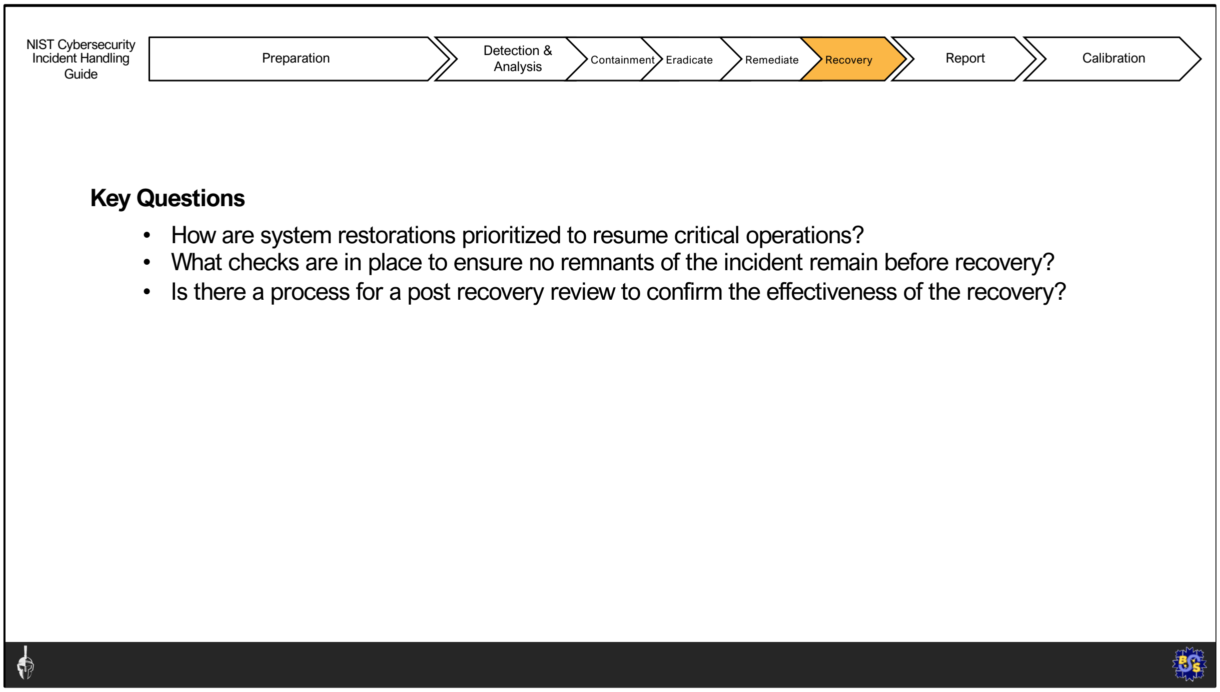
Remediation

We call this step out in the technical IRP which is somewhat unique from the NIST standard for practical reasons. If your team goes through the process of understanding how someone is attacking you and you simply reset your environment as if this hadn’t happened, but don’t prevent it from reoccurring, well, it will reoccur. This critical step therefore focuses on the immediate feedback the technical team can provide as to the root cause of the incident and creates a remediation strategy that is designed to stop the attack before the environment is restored. As a leader this may be highly relevant to you because if the original source of the incident is a service or technical condition that can’t be easily fixed, it may mean that you need to accept working in a degraded state in order to prevent recurrence. It is important that you have clear communication with your technical team in this initial remediation step to shorten the length of the incident and balance competing requirements to restore service.

• Addressing the root cause of the incident to prevent recurrence.
• Implementing improvements to policies, procedures, and technologies based on lessons learned.

- *Conducting a thorough investigation to understand the incident and its implications fully.*

- *Updating the incident response plan to incorporate new insights and strategies.*



NIST Cybersecurity Incident Handling Guide

Preparation

Detection & Analysis

Containment

Eradicate

Remediate

Recovery

Report

Calibration

Key Questions

- How are system restorations prioritized to resume critical operations?
- What checks are in place to ensure no remnants of the incident remain before recovery?
- Is there a process for a post recovery review to confirm the effectiveness of the recovery?

Recovery

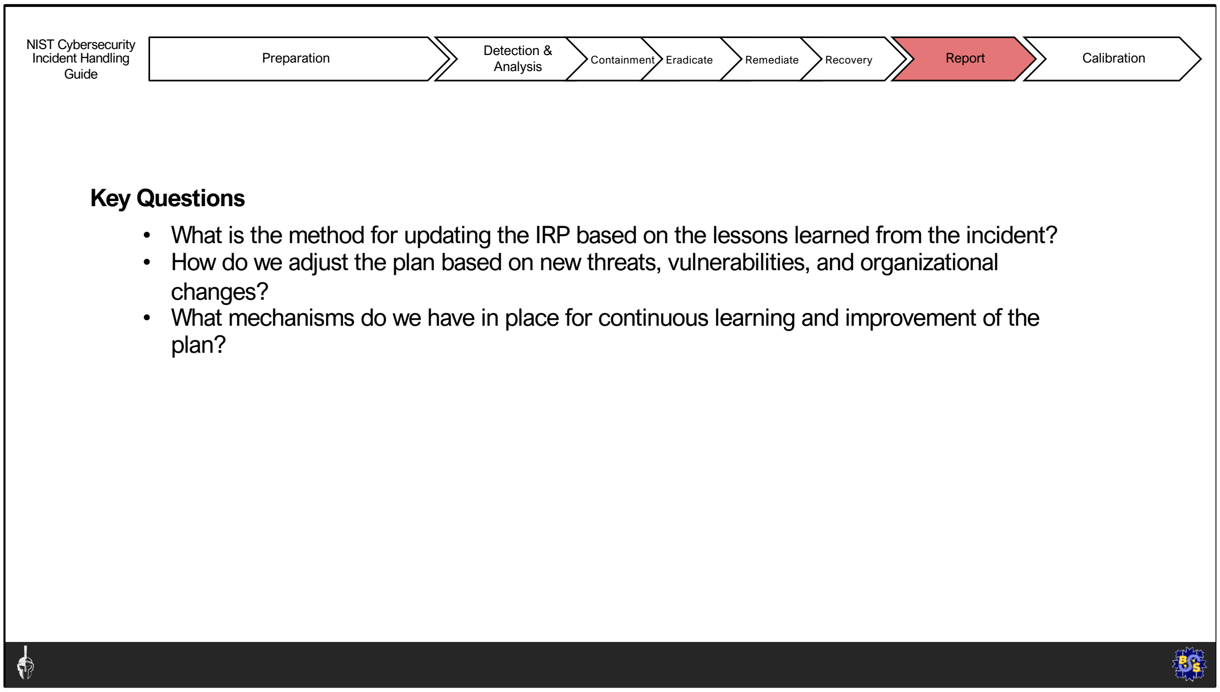
In the recovery step, the primary focus is very similar to a business continuation or disaster recovery plan. The primary goal is to bring affected systems back to a normal operational state. If your work during the prior steps was done correctly, this should be a straightforward set of steps that are performed. From an executive perspective, the most important aspect of recovery is prioritizing team activities to bring the most critical systems back based on your internal processes. The recovery decision being made during this phase is primarily focused on this prioritization and should be seen as an external process within that BCP or DR process. During this phase, the Technical IRP team should be both looking for any signs that the incident wasn't entirely addressed and that there are additional steps in the prior phases as well as

preparing for a post-incident analysis where forensic and root cause analysis can occur.

- *Restoring and returning affected systems and services to normal operation.*
- *Monitoring for any signs of the incident reoccurring as systems return online.*
- *Implementing additional defenses as needed to protect against future*

incidents.

- *Conducting a post-recovery review to ensure that the recovery was complete and effective.*



NIST Cybersecurity Incident Handling Guide

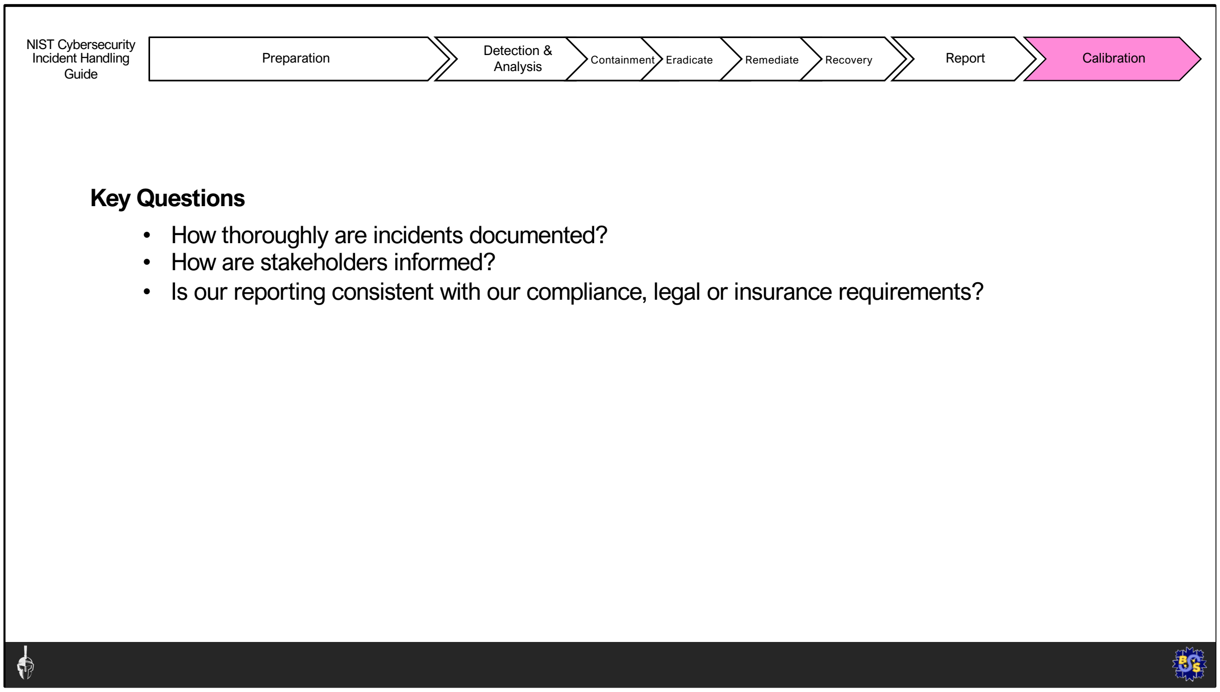
Preparation
Detection & Analysis
Containment
Eradicate
Remediate
Recovery
Report
Calibration

Key Questions

- What is the method for updating the IRP based on the lessons learned from the incident?
- How do we adjust the plan based on new threats, vulnerabilities, and organizational changes?
- What mechanisms do we have in place for continuous learning and improvement of the plan?

Reporting
• Documenting the incident's details, including how it was detected, the response actions taken, and the lessons learned.
• Reporting to relevant stakeholders, which may include internal management or external agencies, depending on the incident's nature and impact.
• Ensuring compliance with any legal or regulatory reporting requirements.
• Using the report to improve future incident response efforts and organizational security posture.

Calibration
• Reviewing and adjusting the incident response plan and processes based on current threats, vulnerabilities, and organizational changes.
• Continuously learning from incidents and incorporating feedback into the incident response lifecycle.
• Testing and exercising the incident response plan to ensure its effectiveness and team readiness.
• Keeping the incident response team's skills



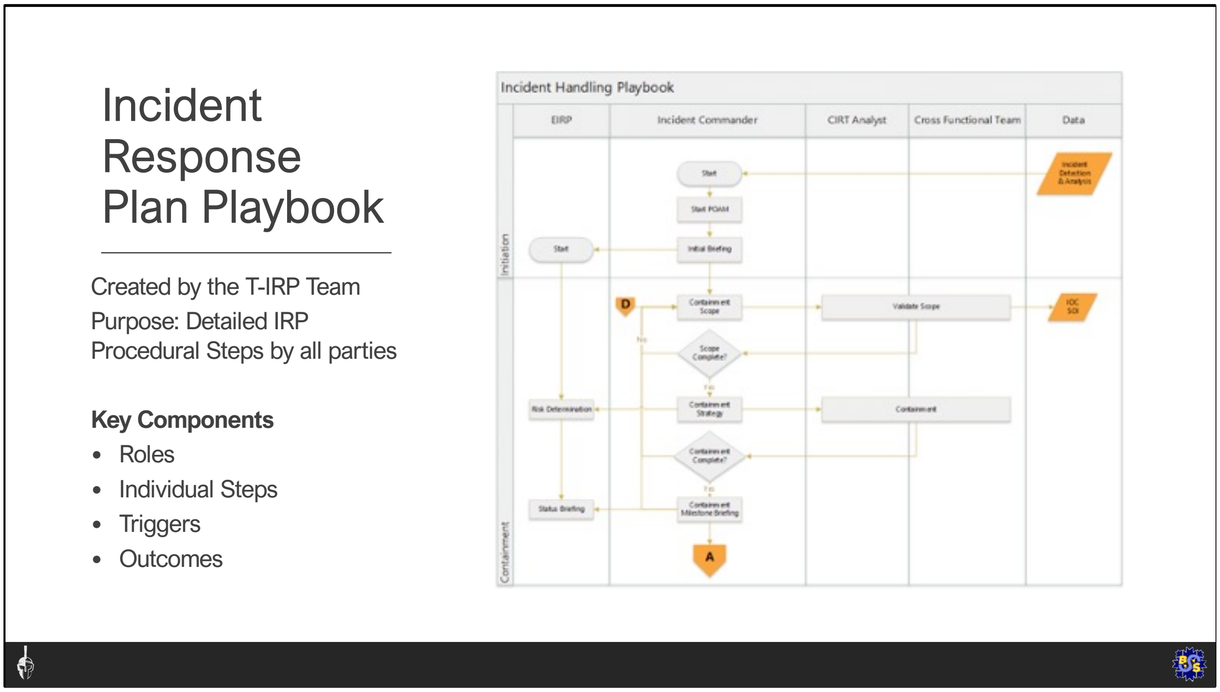
NIST Cybersecurity Incident Handling Guide

Preparation → Detection & Analysis → Containment → Eradicate → Remediate → Recovery → Report → Calibration

Key Questions

- How thoroughly are incidents documented?
- How are stakeholders informed?
- Is our reporting consistent with our compliance, legal or insurance requirements?

Calibration
• Reviewing and adjusting the incident response plan and processes based on current threats, vulnerabilities, and organizational changes.
• Continuously learning from incidents and incorporating feedback into the incident response lifecycle.
• Testing and exercising the incident response plan to ensure its effectiveness and team readiness.
• Keeping the incident response team's skills



Incident Response Plan Playbook

Created by the T-IRP Team

Purpose: Detailed IRP Procedural Steps by all parties

Key Components

- Roles
- Individual Steps
- Triggers
- Outcomes

An Incident Response Playbook is a detailed, step-by-step guide designed to manage and resolve incidents efficiently and effectively. It is based on the broader Incident Response Plan, which sets out the overall strategy for handling incidents. The playbook operationalizes this plan by providing specific procedures for different types of incidents. Below is an outline of an Incident Response Playbook, including role definitions and how it integrates with the overall plan:

Outline

- *Key Role Definitions, including the Incident Commander, Analyst, and Cross Functional Teams*
- *Specific activities that define how the Incident Commander will request and coordinate the services of all teams*
- *Develops and supports the POAM which documents and advances the incident response*

Summary of Goals

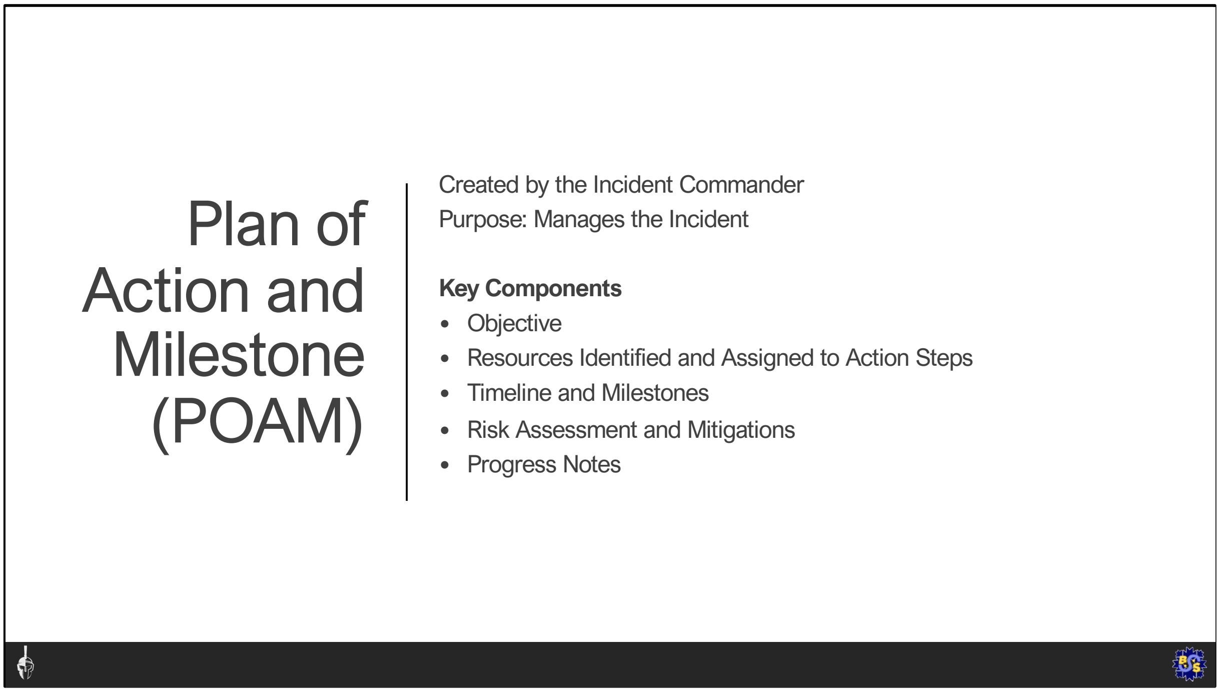
- *Provide a clear, actionable guide for responding to various types of incidents.*
- *Ensure quick and effective instructions to teams as to role, and specific*

actions that can be taken

Key Questions

- *Does the playbook cover a wide range of potential incidents?*
- *Are the roles and responsibilities clearly defined and understood?*
- *Is there a clear process for incident detection, reporting, and assessment?*
- *Are the response steps practical and actionable?*
- *Does the playbook include protocols for communication, both internally and externally?*
- *Are there procedures for post-incident analysis and reporting?*
- *Does the playbook provide a framework for continual improvement based on incident data?*
- *Are the tools and resources required for incident response identified and readily available?*
- *Is there a clear linkage between the playbook procedures and the broader Incident Response Plan?*
- *Does the playbook include considerations for legal, regulatory, and compliance aspects?*

The effectiveness of an Incident Response Playbook lies in its ability to operationalize the Incident Response Plan, guiding the organization through the complexities of incident management and ensuring resilience in the face of security threats.



Plan of Action and Milestone (POAM)

Created by the Incident Commander

Purpose: Manages the Incident

Key Components

- Objective
- Resources Identified and Assigned to Action Steps
- Timeline and Milestones
- Risk Assessment and Mitigations
- Progress Notes

Creating a Plan of Action and Milestone (POAM) is a structured approach to achieving specific goals within a defined timeframe. The purpose of a POAM is to outline the steps required to accomplish objectives, identify necessary resources, and set clear milestones for tracking progress. Here's a summary and key elements to include in a POAM:

Summary

• Objective Definition: Clearly define what you aim to achieve. This should be specific, measurable, achievable, relevant, and time-bound (SMART).

• Resource Identification: List the resources (people, money, equipment, etc.) necessary to achieve the objectives.

• Action Steps: Break down the objective into smaller, manageable tasks or action steps.

• Timeline Establishment: Set a realistic timeline for each action step, including start and end dates.

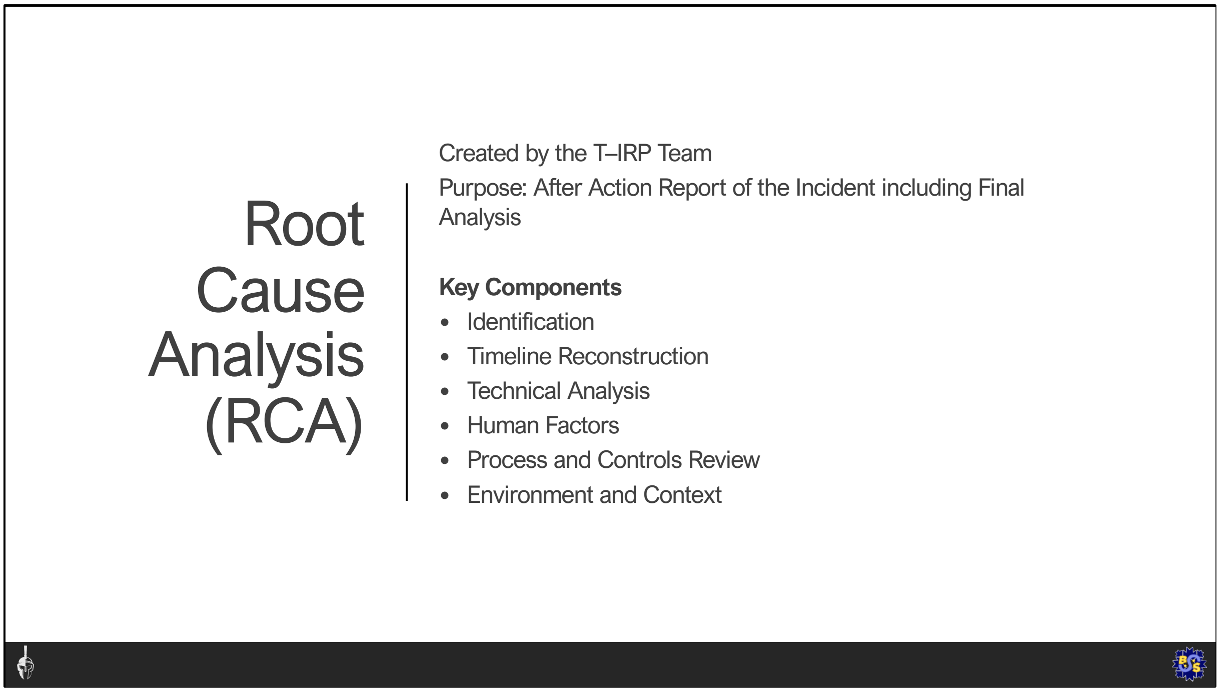
• Milestone Creation: Establish key milestones that act as checkpoints to track progress towards the objective.

• Responsibility Assignment: Assign specific tasks to individuals or teams, making sure everyone knows their roles and responsibilities.

• Risk Assessment and Mitigation: Identify potential risks or obstacles and plan how to address them.
• Progress Monitoring and Adjustment: Regularly review progress, update the POAM as necessary, and make adjustments to stay on track.
• Final Evaluation: Assess the overall success of the project upon completion and identify lessons learned for future endeavors.

Key Questions
• Is the objective SMART? (Specific, Measurable, Achievable, Relevant, Time-bound)
• Are the required resources clearly identified and available?
• Are the action steps practical and broken down into manageable tasks?
• Is the timeline realistic and does it include buffer periods for unforeseen delays?
• Do the milestones effectively measure progress towards the objective?
• Are responsibilities clearly assigned and understood by all team members?
• Have potential risks been identified and mitigation plans put in place?
• Is there a robust system for monitoring progress and addressing issues promptly?
• Are there procedures for making adjustments to the plan as needed?
• How will the success of the project be evaluated and what are the criteria for success?

A well-constructed POAM not only guides the project through its lifecycle but also ensures alignment with strategic objectives, effective resource utilization, and adaptability to changes and challenges.



Root Cause Analysis (RCA)

Created by the T–IRP Team

Purpose: After Action Report of the Incident including Final Analysis

Key Components

- Identification
- Timeline Reconstruction
- Technical Analysis
- Human Factors
- Process and Controls Review
- Environment and Context

Cybersecurity incident root cause analysis (RCA) is a deep dive into understanding the fundamental reasons why a particular security breach or incident occurred. The goal is to not just address the symptoms of the breach, but to uncover and resolve underlying issues to prevent future incidents. This process involves a thorough examination of the incident, typically following a structured methodology to identify both the technical causes and the human or process-related factors that led to the incident. RCA is essential for improving an organization's security posture and resilience against cyber threats.

Key Points:
• Identification: Accurately identifying and describing the cybersecurity incident, including its scope and impact.
• Timeline Reconstruction: Establishing a timeline of events leading up to, during, and after the incident to understand the sequence of actions.
• Technical Analysis: Examining the technical aspects of the incident, such as vulnerabilities exploited, malware used, or system failures.
• Human Factors: Assessing any human elements, including errors, oversights, or actions that may have contributed to the incident.
• Process and Controls Review: Evaluating the adequacy of existing processes

and controls that should have prevented the incident.

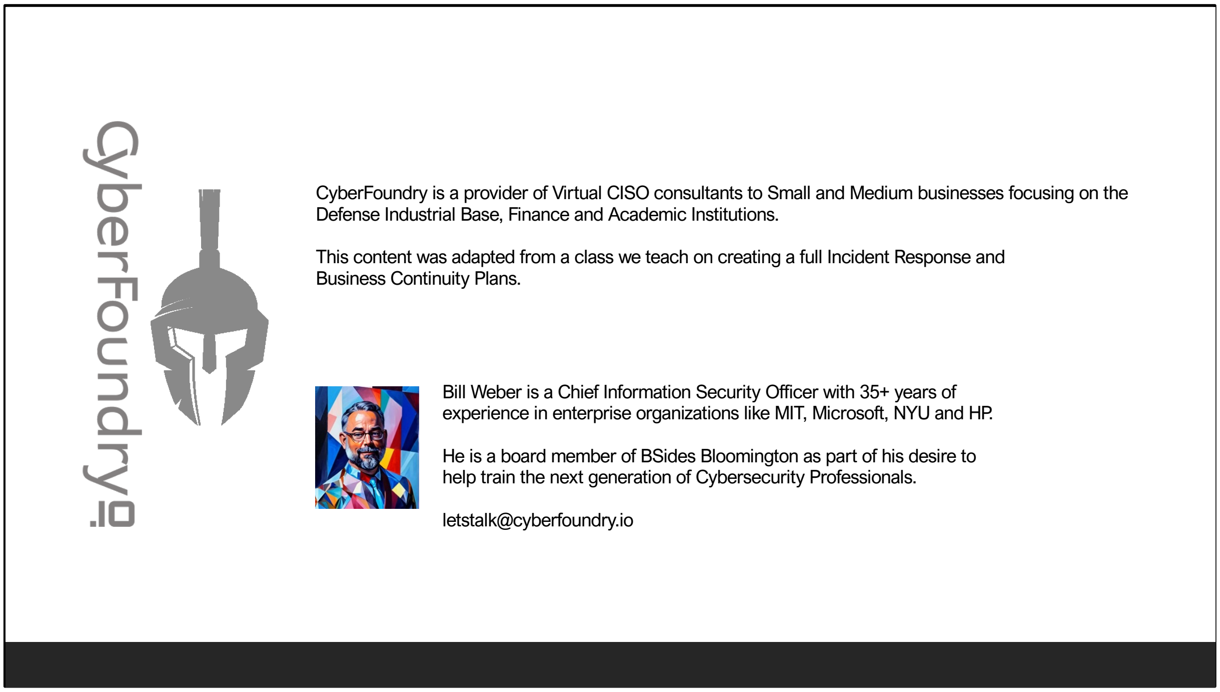
- *Environment and Context: Considering external factors such as the current threat landscape or relevant industry trends that could have influenced the incident.*

Key Questions:

- *What specific vulnerabilities or failures allowed the incident to occur?*
- *Were there any warning signs or precursors that were missed?*
- *What sequence of events led to the incident?*
- *Which processes, policies, or controls failed or were absent?*
- *Who was involved, and what were the human factors contributing to the incident?*
- *How did the organizational culture or environment play a role in the incident?*
- *What can be learned from this incident, and how can we prevent similar incidents in the future?*

Root cause analysis is critical for closing security gaps and enhancing an organization's defenses, ensuring that measures are taken not only to correct the immediate issue but also to prevent recurrence.

NOTE: This should not become a public document. It will contain sensitive information that is not necessary to disclose.



CyberFoundry is a provider of Virtual CISO consultants to Small and Medium businesses focusing on the Defense Industrial Base, Finance and Academic Institutions.

This content was adapted from a class we teach on creating a full Incident Response and Business Continuity Plans.

Bill Weber is a Chief Information Security Officer with 35+ years of experience in enterprise organizations like MIT, Microsoft, NYU and HP.

He is a board member of BSides Bloomington as part of his desire to help train the next generation of Cybersecurity Professionals.

letstalk@cyberfoundry.io