# Incident Response Workshop

CyberFoundry

**Join at slido.com**
**#3418410**

# Your Presenters

**Ken Michael** has spent four decades building Dox Electronics into a fortress against cyber threats. A stack of security certifications proves he knows how to keep businesses safe—though some say he just enjoys making auditors nervous.

When night falls, Ken trades firewalls for camera lenses. He's usually out taking photos of the dark, which makes sense—his best shots are the ones where absolutely nothing can be seen. Some people chase the light; Ken prefers to hunt the shadows.

**Bill Weber** has spent decades turning complex security problems into workable plans for enterprises, defense programs, and anyone brave enough to ask for help. A career CISO, he's navigated compliance minefields, government audits, and the occasional corporate meltdown—usually without setting the building on fire.

CyberFoundry

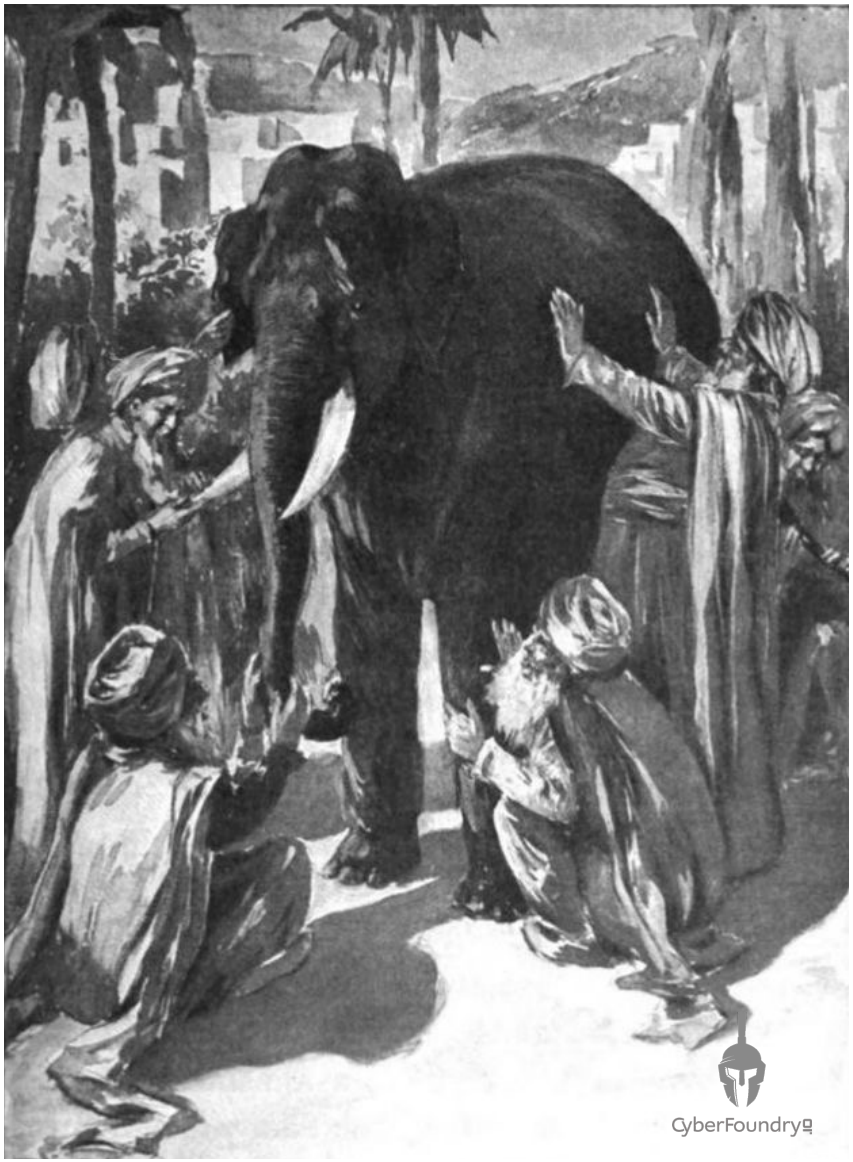
# agenda

**Part 1**
**Understanding the Incident Response Plan**

**Part 2**
**Tabletop Exercise**

# Part 1

## Understanding the Incident Response Plan



# First Principals

***Cybersecurity First Principal***

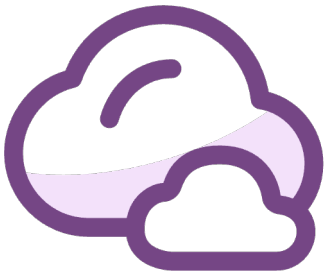
*“Reduce the probability of material impact due to a cyber event over the next three years.”*

*- Ron Howard*

***Incident Response First Principal***

*“Detect, contain, and remediate incidents in ways which reduce the probability and scale of a material impact.”*

*-Bill Weber*



# When you hear “cyber Incident”, what’s the first think you think of loosing?

# What does an incident look like?

# So, What Qualifies as an Incident?

**This is not an IT problem.**
This is a **$X/day production loss**, **$Y in contractual penalties**, and **risk to $Z in long-term revenue** if compliance is breached.

**Operational Loss**
Factory Shutdown → every day offline = $X in lost production.

**Financial Loss**
Direct costs: ransom demand, forensics, legal fees, overtime.
Indirect costs: penalties for missed SLAs, lost contracts.

**Data & IP Loss**
Loss of proprietary designs, formulas, or trade secrets.
Exposure of customer or regulated data → regulatory fines.

**Reputational Loss**
Customers lose confidence, stock dips, trust erodes.

**Compliance / Legal Loss**
Fines from GDPR, HIPAA, SEC, FTC.


"... the plant shut down about an hour ago.

Some message about being encrypted until we pay,
so, we called you.

Can you fix it?"

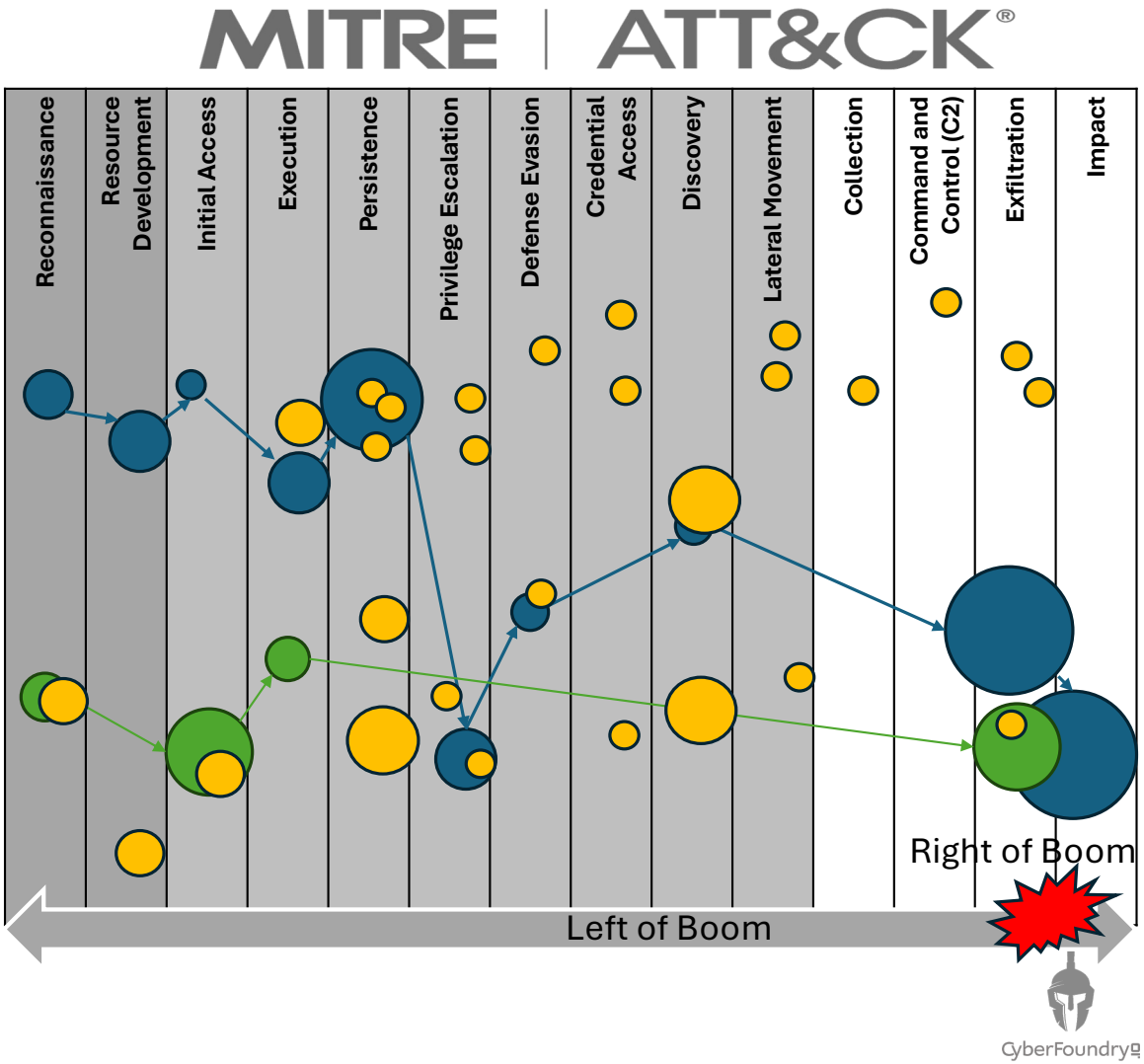
CyberFoundry

# What does an attack look like?

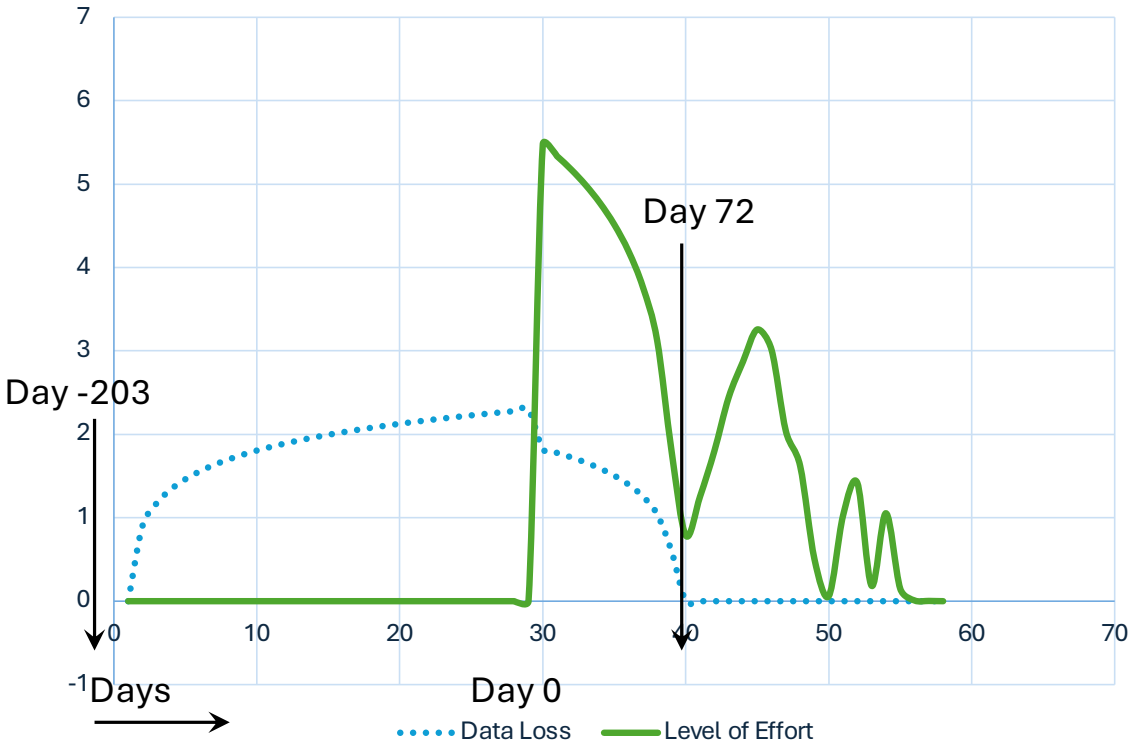
Questions:

Here are three very different attack signatures.

- which one would be the hardest to defend against?
- Which one generated the largest potential material impact?



# When do losses occur?





CyberFoundry

What is an incident response plan?

# The Standards

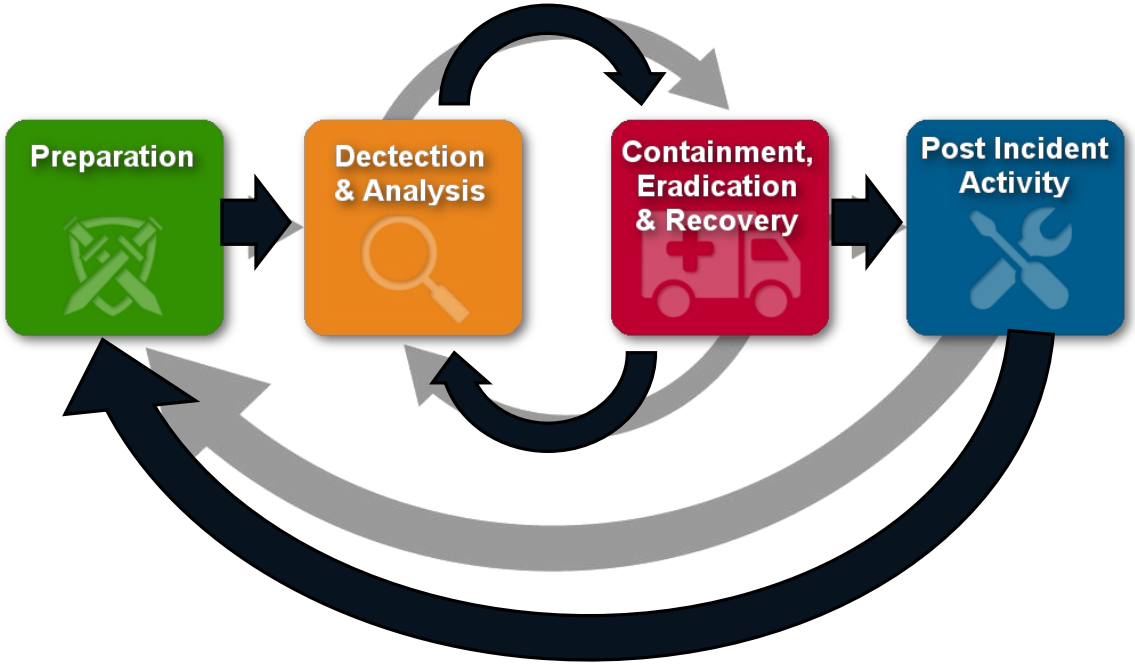
# Cybersecurity Framework 2.0

For Industry, Government, and Organizations to Reduce. Cybersecurity Risks


CyberFoundry

# Computer Security Incident Handling Guide
# NIST SP800-61r2

Industry Standard
Cyber Incident
Response Cycle




CyberFoundry

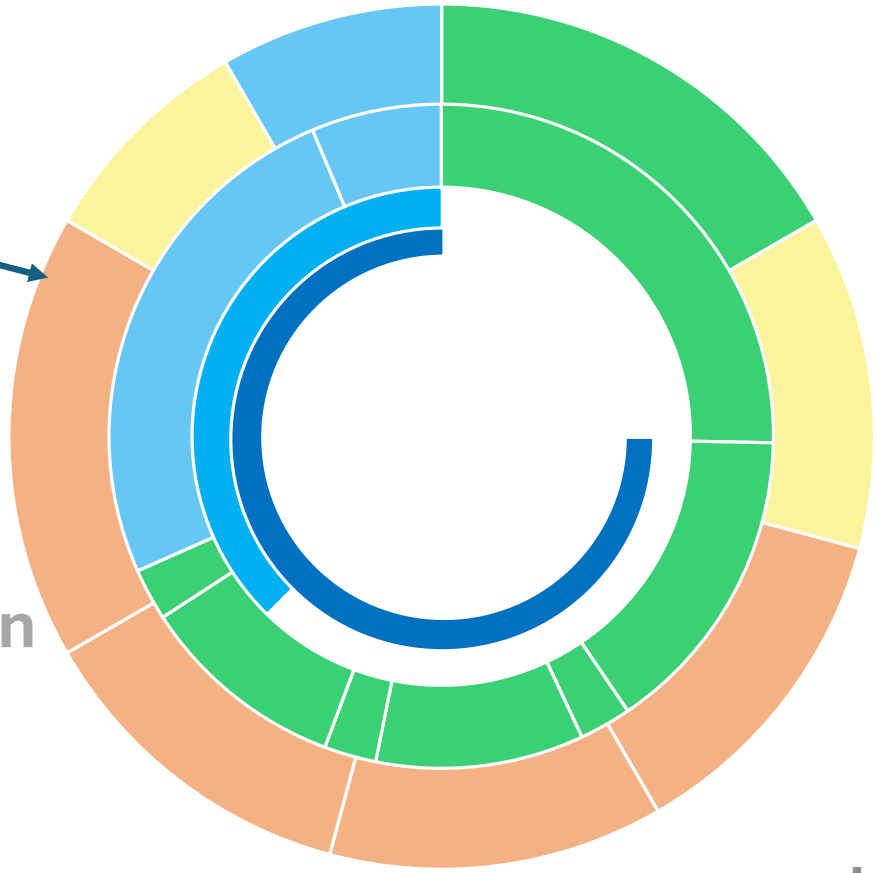
# Cyber Foundry Incident Response Plan

# Anatomy of an Incident Response Plan (IRP)

- **TIRP - Technical IRP**
  Put the fire out.

- **EIRP - Executive IRP**
  Decide which building to save first.

- **CMP - Crisis Management Plan**
  Explain to the city why the neighborhood is on fire.



CyberFoundry

# The Characters

# Incident Commander

- Owns and makes all decisions regarding the technical response to the incident
- Supports the executive and crisis management teams
- Keeps the swim lanes separate
- Could be the CISO, or someone from the Incident Response Team

CyberFoundry

# Incident Response Team (IRT) / SOC

- Leads the implementation of the technical incident response plan steps under leadership of the incident commander.
- Collaborates with the other teams to execute and validate changes in the environment.

## IT / Business Support

- Leads changes to the IT environment necessary to contain, eradicate and recover from an incident.
- Closest to the business impact and the users.

## Executive Sponsor

- Responsible for engagement of the Senior Leaders and for their actions to reduce the impact once a loss occurs.

# General Council Crisis Manager

- Responsible for maintaining attorney client privilege over all evidence.
- Responsible for communicating with regulators, law enforcement, insurers, investors and the media.
- Enforce separation of duties.

# Let's Summarize

| | TIRP | EIRP | CMP |
|---|---|---|---|
| **Incident Commander** | A/R - Declares Incidents, Owns Coordination, Makes Technical Decisions | A/R - Bridges Business Risk to Technical Plan, Prioritizes Service Recovery, Provide TIRP Status | S – Provides CS Status |
| **Incident Response Team** | R – Detect, analyze, contain, eradicate. Root Cause Analysis | I – Informed of decisions that affect TIRP | I – Informed of. Decisions that affect TIRP |
| **IT/Business** | S/R – Supports containment, restores systems | I – Provides IT status | I – Provide IT Status |
| **General Council / Crisis Manager** | C – Advice on evidence handling. | C/R – Ensure compliance, manage disclosure obligations. | A/R – Manage regulators, law enforcement, insurers; preserve privilege. |
| **Executive Sponsor** | I – Briefed on process and outcome | A/R – Make risk and continuity decisions. | S – Support crisis comms and continuity decisions. |

**(R)esponsible**
**(A)ccountable**
**(S)takeholder**
**(C)onsulted**
**(I)nformed**

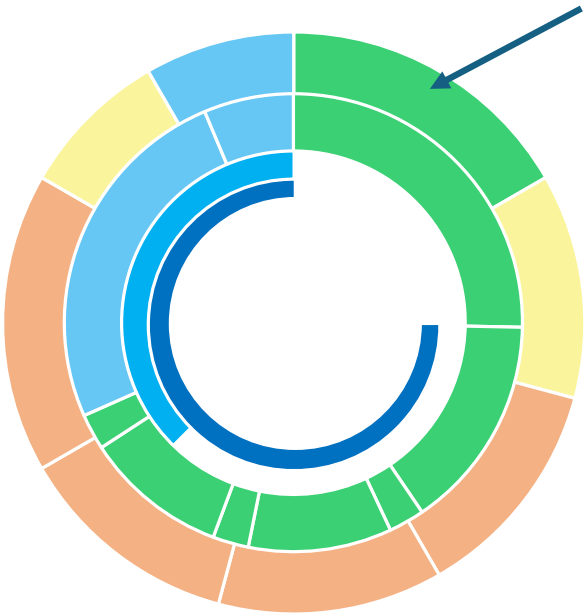
CyberFoundry

# Technical Incident Response Plan

Objectives

- Rapid Detection & Assessment
- Effective Containment & Mitigation
- Eradication & Recovery
- Learning & Improvement
- Impact Reduction

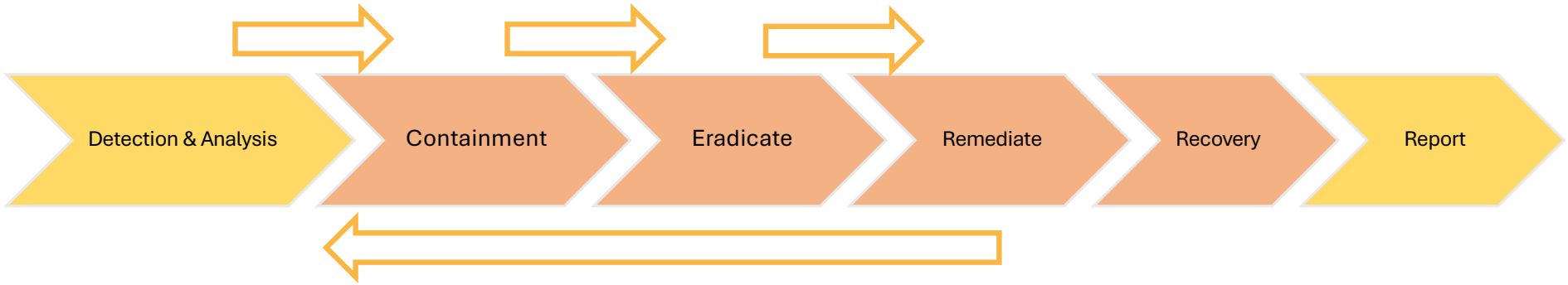
# Technical Incident Response Plan Process

- **Preparation**
  *Build the people, processes, and tools you'll need before an incident strikes.*
- **Detection & Analysis**
  *Identify and validate that an event is happening, and assess its scope and impact.*
- **Containment**
  *Limit the damage by isolating affected systems and preventing further spread.*
- **Eradication**
  *Remove the attacker's foothold, malware, and vulnerabilities from the environment.*
- **Remediation**
  *Fix the root causes that allowed the incident, strengthening defenses against recurrence.*
- **Recovery**
  *Restore systems and business operations to normal, carefully and securely.*
- **Report**
  *Document what happened, what actions were taken, and communicate to stakeholders.*
- **Calibration**
  *Refine and improve the IR plan through lessons learned and regular exercises.*

CyberFoundry

# Gates & Continuous Validation




Every Phase has an Entry set of Actions and an Exit set of Criteria.
If these Gates are found to not have been completed, then action must go back to the previous phase.

**Examples:**

- The Detection & Analysis phase indicated an incomplete scope which was later detected during Eradication.
- The Eradication phase missed an impacted system which was later detected during Recovery.
- An Indicator of Compromise (IOC) was identified in the Containment phase but not acted on.
  This was detected when writing up the final report.

CyberFoundry

# Phase Gates

| Phase | Incoming Gate | Exit Gate |
|---|---|---|
| **Preparation** | - IRP approved and current<br>- Contact list and escalation paths validated<br>- Tools / Playbooks tested and available | - Team trained and exercised<br>- Baseline monitoring in place<br>- Evidence handling procedures documented |
| **Detection & Analysis** | - Monitoring / logging active<br>- Incident criteria (classification matrix) ready | - Incident ticket created with initial classification<br>- Scope defined and validated<br>- Do we know enough to move into containment? |
| **Containment** | - Confirmed incident scope<br>- Stakeholders notified and potential operational impacts identified<br>- Incident Response Plan initiated via Incident Commander | - Systems isolated, blocked, or segmented as defined<br>- Containment effectiveness validated |
| **Eradication** | - Confirmed containment in place<br>- Known attack artifacts catalogued | - Malicious artifacts removed or neutralized<br>- Systems patched / vulnerabilities remediated<br>- Independent validation scan / forensic check completed |
| **Recovery** | - Eradication confirmed successful / no active compromise remains<br>- Recovery procedures tested in staging (if possible) | - Systems restored and validated operationally<br>- Monitoring intensified to detect reoccurrence<br>- Stakeholders notified of recovery status |
| **Reporting** | - Incident records complete (investigation log, eradication, recovery evidence)<br>- Legal / regulatory obligations identified | - Notifications filed (internal, external, regulatory)<br>- Root Cause Analysis (RCA) drafted<br>- Incident formally closed |
| **Calibration / Lessons Learned** | - Incident report available<br>- Stakeholders scheduled for review session | - Root Cause Analysis finalized<br>- Lessons Learned documented and distributed<br>- IRP/Playbooks updated / training & exercises planned or revised |

CyberFoundry

# Run Books vs. Procedures

## Run Books

Scenario-specific playbook that stitches together multiple procedures into an end-to-end response workflow for a particular incident type.

- Scenario Based (e.g. Ransomware infection)
- Guides responder through the entire IRP Plan
- Contains conditional logic focusing on the full recipe

## Examples:

- Ransomware IRP Playbook
- Lost laptop IRP Playbook

## Procedures

Generic, reusable blocks that describe how to perform a specific task or operation in a consistent, repeatable way.

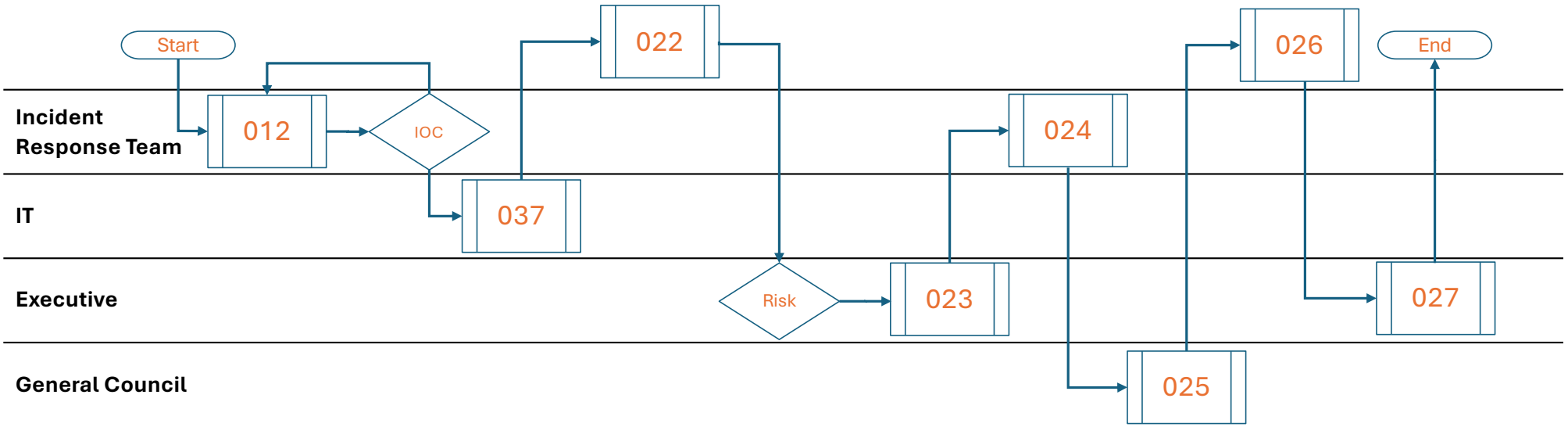
- Narrow and task-focused
- Standardized reusable build blocks
- Step-by-step, tool specific

## Examples:

- Change User Password
- Erase and Image a Laptop Image

CyberFoundry

# Run Books vs. Procedures Example



# Let's Review

| | TIRP | EIRP | CMP |
|---|---|---|---|
| **Incident Commander** | A/R - Declares Incidents, Owns Coordination, Makes Technical Decisions | A/R - Bridges Business Risk to Technical Plan, Prioritizes Service Recovery, Provide TIRP Status | S – Provides CS Status |
| **Incident Response Team** | R – Detect, analyze, contain, eradicate. Root Cause Analysis | I – Informed of decisions that affect TIRP | I – Informed of. Decisions that affect TIRP |
| **IT/Business** | S/R – Supports containment, restores systems | I – Provides IT status | I – Provide IT Status |
| **General Council / Crisis Manager** | C – Advice on evidence handling. | C/R – Ensure compliance, manage disclosure obligations. | A/R – Manage regulators, law enforcement, insurers; preserve privilege. |
| **Executive Sponsor** | I – Briefed on process and outcome | A/R – Make risk and continuity decisions. | S – Support crisis comms and continuity decisions. |

**(R)esponsible**
**(A)ccountable**
**(S)takeholder**
**(C)onsulted**
**(I)nformed**

CyberFoundry


## Key Questions:

- Do we have the necessary 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?

### Key Deliverables:

Incident Response Policy / Plan

- Roles & Responsibilities RASCI
- Communications & Escalation Plan
- TIRP, EIRP and Crisis Management Plans

### Other Key Deliverables:

- Authoritative Asset & Data Inventory
- Business Impact Analysis & Criticality Register
- Vulnerability & Patch Management
- Tooling & Telemetry Readiness
- Detection / Threat Model Use-Cases
- Backup & Recovery Plans
- Forensic Handling Standard Operating Procedure (SOP)
- Third Party Risk Management Plan
- Performance Baseline

CyberFoundry


## 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?

## Key Deliverables:

- Incident Detection Log / Alert Record
- Incident Classification / Severity Report
- Scope & Impact Assessment
- Evidence Preservation Process

CyberFoundry


## Key Questions:

- What strategies are implemented 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?

## Key Deliverables:

- Containment playbooks / strategy
- Containment action log
- Stakeholder communication record
- Evidence Preservation Package

CyberFoundry


## 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?
- Are eradication efforts designed to be compliant with legal and regulatory requirements?

## Key Deliverables:

- Interim Root Cause Analysis
- Artifact & Persistence Removal Log
- Vulnerability Remediation Log
- Eradication Validation Results

CyberFoundry


## Key Questions:

- How do we confirm that all known indicators of compromise have been eliminated across affected systems?
- What additional hunting or validation steps are needed to ensure there are no undetected compromises?
- Are containment and eradication measures still holding, and have any new anomalies been observed?
- Who provides the formal “all clear” signal that authorizes the transition into recovery?

## Key Deliverables:

- IOC Validation Report
- Threat-Hunting Summary
- Residual Risk Assessment
- All Clear Authorization

CyberFoundry


## Key Questions:

- What systems and services must be restored first to minimize business disruption?
- How do we ensure that restored systems are clean, trustworthy, and not reinfected?
- What additional monitoring is in place to detect signs of recurrence during recovery?
- Are recovery activities aligned with business continuity and disaster recovery plans?
- Who authorizes the return of systems to production and at what thresholds?
- What safeguards or compensating controls are required until full remediation is achieved?
- How do we validate recovery success across business and technical stakeholders?

## Key Deliverables:

- Recovery Prioritization Plan
- Restoration Log
- Clean-State Validation Results
- Enhanced Monitoring Report
- Recovery Authorization Sign-Off
- Post-Recovery Review Notes

CyberFoundry


## Key Questions:

- What are the complete details of the incident, including timeline, detection, actions taken, and resolution?
- How do we ensure compliance with legal, regulatory, and contractual reporting requirements?
- Who are the relevant stakeholders, and how is the incident communicated to each of them?
- What lessons can be drawn from the incident to improve future response?

## Key Deliverables:

- Incident Summary Report
- Regulatory & Compliance Report Pack
- Stakeholder Communication Pack
- Incident Action & Decision Log
- Lessons Learned Report / Root Cause Analysis

CyberFoundry


## Key Questions:

- How did our incident response policies, processes, and playbooks perform, and where did they fail?
- What improvements must be made to detection, containment, eradication, remediation, and recovery procedures?
- How do we incorporate root cause findings and lessons learned into future readiness?
- Have compliance, legal, or contractual obligations highlighted new requirements for the plan?
- When and how will the revised plan be tested to validate effectiveness and team readiness?
- What skills, tools, or training does the response team need to improve before the next incident?

## Key Deliverables:

- TIRP Update Package
- Gap Analysis & Improvement Plan
- Updated RCA & Lessons Integration
- Exercise & Testing Results
- Training & Skills Development Plan
- Executive / Board Calibration Brief

CyberFoundry

# Technical Incident Response Plan Documentation

| Phase | Reference / Input Document | Generated / Output Document |
|---|---|---|
| **Preparation** | - Incident Response Policy - Incident Classification Matrix - Playbooks / Runbooks - Communication Plan - Contact Lists - System & Network Documentation - Legal & Regulatory Obligations - Evidence Handling Procedures | - Tabletop Exercise / Training Records |
| **Detection & Analysis** | - Classification Matrix - Playbooks (by incident type)<br>- Logging/Monitoring Standard | - Initial Incident Report / Ticket - Investigation Log (chronological notes, evidence references)<br>- Situation Reports (SitReps) for stakeholders |
| **Containment** | - Containment Playbooks - System Documentation (dependencies, critical systems) | - Containment Records (what was isolated/blocked, when, by whom)<br>- Updated SitReps |
| **Eradication** | - Malware Removal Procedures - Vendor/Forensics SOPs | - Eradication Records (removed accounts, deleted malicious files, patched systems) |
| **Recovery** | - System & Network Documentation - Recovery Procedures (restore, rebuild, validate) | - Recovery Validation Report (evidence systems are clean, back to baseline)<br>- Final SitRep |
| **Reporting** | - Communication Plan - Legal/Regulatory Obligations | - Regulatory/Stakeholder Notifications - External Reports (customers, partners, law enforcement) |
| **Calibration / Lessons Learned** | - Evidence Handling Procedures (for RCA) - Compliance / Framework Mappings (NIST, ISO, etc.) | - Root Cause Analysis (RCA)<br>- Lessons Learned Report<br>- Calibrated IRP Update (revised playbooks/policies) |

# Executive Incident Response Plan

Objectives

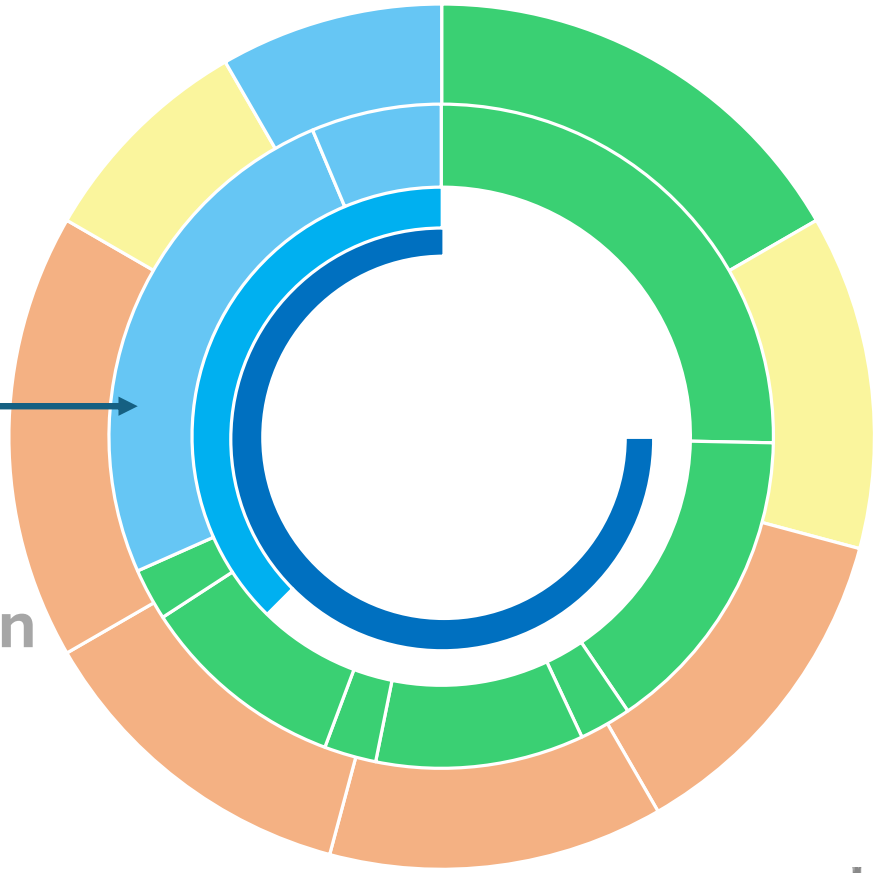
- Reduce the material impact to the business from a cybersecurity incident
- Inform the business, stakeholders and officials

# Anatomy of an Incident Response Plan (IRP)

- **TIRP - Technical IRP**
  Put the fire out.

- **EIRP - Executive IRP**
  Decide which building to save first.

- **CMP - Crisis Management Plan**
  Explain to the city why the neighborhood is on fire.



CyberFoundry

# Technical Incident Response Plan



# Executive Incident Response Plan


CyberFoundry

# Let's Summarize

| | TIRP | EIRP | CMP |
|---|---|---|---|
| **Incident Commander** | A/R - Declares Incidents, Owns Coordination, Makes Technical Decisions | A/R - Bridges Business Risk to Technical Plan, Prioritizes Service Recovery, Provide TIRP Status | S – Provides CS Status |
| **Incident Response Team** | R – Detect, analyze, contain, eradicate. Root Cause Analysis | I – Informed of decisions that affect TIRP | I – Informed of. Decisions that affect TIRP |
| **IT/Business** | S/R – Supports containment, restores systems | I – Provides IT status | I – Provide IT Status |
| **General Council / Crisis Manager** | C – Advice on evidence handling. | C/R – Ensure compliance, manage disclosure obligations. | A/R – Manage regulators, law enforcement, insurers; preserve privilege. |
| **Executive Sponsor** | I – Briefed on process and outcome | A/R – Make risk and continuity decisions. | S – Support crisis comms and continuity decisions. |

**(R)esponsible**
**(A)ccountable**
**(S)takeholder**
**(C)onsulted**
**(I)nformed**

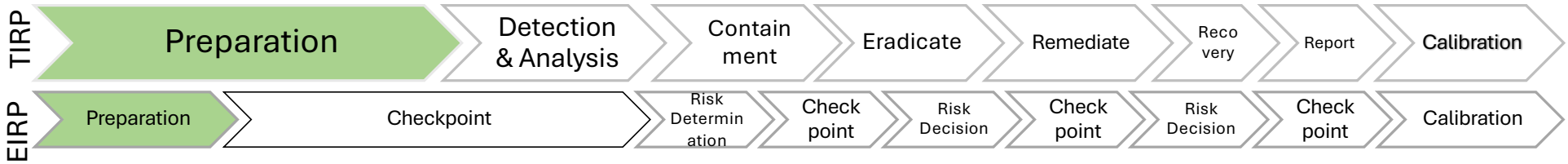
CyberFoundry

# Phase Gates

| Phase | Incoming Gate | Exit Gate |
|---|---|---|
| **Preparation** | Current BIA, risk appetite, RTO/RPO/SLOs, insurance and regulatory playbooks, comms templates, role roster, IC authority defined. | Exec roles/thresholds confirmed; IC empowered to convene EIRP; business priorities (“crown jewels”) and downtime tolerances re-affirmed. |
| **Checkpoint** | IC summary of facts/unknowns, preliminary blast radius, safety status, early exfil signal, evidence-preservation posture. | Preliminary materiality hypothesis; cadence for IC briefings; GC activates compliance/insurance review; direction to preserve evidence. |
| **Risk Determination** | D&A findings: likely access vector, attacker objectives (if known), confirmed impacted systems/lines/sites, spread risk, safety impacts, exfil yes/no, containment options (scoped). | Business impact level (operational/financial/compliance/reputational) set.<br>Containment objectives approved (what to isolate/shut down; plant/partner cutovers aligned to BIA).<br>Downtime SLOs and “must-keep-running” services stated.<br>Direction on internal/partner notifications and holding statement.<br>IC authorized to execute the chosen containment posture. |
| **Checkpoint** | Containment progress, residual spread risk, any dependency hits (ERP/MES/AD), safety status, early media/partner pressure. | Confirm containment scope holds; adjust business comms if needed; greenlight prep of eradication options package. |
| **Risk Decision 1** | Eradication plan with options and impacts: wipe/reimage scale, evidentiary implications, expected downtime extension, clean-build sources, privileged credential resets; ransom intel (if any), insurer and GC guidance, LE/regulator notification status. | Go/no-go on eradication approach (including **authorization to erase/reimage at scale**).<br>Stance on ransom (**default no-pay** unless explicit exception).<br>Evidence-handling constraints and LE engagement confirmed.<br>Acceptance of operational pain to ensure a clean environment; continuity workarounds funded.<br>IC authorized to execute eradication and credential resets. |

# Phase Gates

| Phase | Incoming Gate | Exit Gate |
|---|---|---|
| **Checkpoint** | Eradication status vs. completion criteria, surprises (persistence, new IOCs), evidence status, insurer/regulator asks. | Agreement on “eradicated” definition met; no blockers to begin remediation; prioritize remediation plan draft reviewed for business fit. |
| **Risk Decision 2** | Remediation status (patch/rebuild/hardening complete or near-complete), residual risk register, validation results, **recovery playbook options** (phased waves, partial reopen), resource constraints, backlogs. | Recovery **prioritization** by business process (which systems go first; which remain offline).<br>Go-live criteria, monitoring & rollback thresholds, and staffing coverage approved.<br>Communications plan for employees/customers/partners/regulators set.<br>IC authorized to initiate recovery waves per priority. |
| **Checkpoint** | IC attests technical readiness; BU owners attest operational readiness; comms ready; insurers/regulators alignment OK. | Formal “return-to-service” authorization (partial or full); live monitoring & stabilization window defined; cadence for exec status set. |
| **Calibration** | AARs (TIRP/CMP), cost & downtime metrics, control gaps, insurance/reg feedback. | Adjusted risk appetite/BCP/IRP; funded improvements; board/regulator briefing; scheduled re-tests/tabletops. |



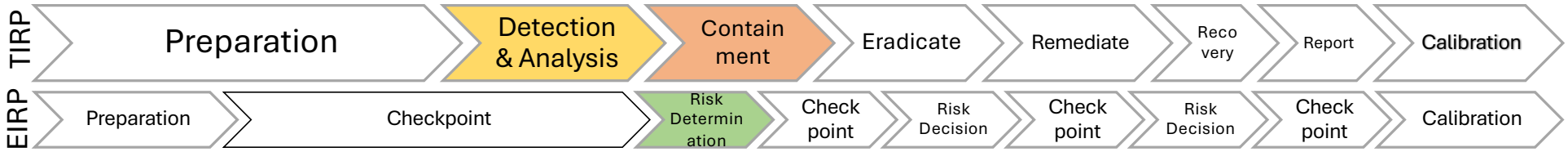

## Key Questions:

- Are roles and authorities clearly defined?
- What's our current risk appetite and downtime tolerance?
- Are BIA and service recovery priorities current?
- Do we understand our compliance, regulatory, and insurance obligations?

## Key Deliverables:

- Executive role roster & decision thresholds.
- Business Impact Analysis (BIA) + recovery SLOs confirmed.
- Insurance and regulator notification playbooks reviewed.
- Communication templates (internal, partners, customers).

CyberFoundry



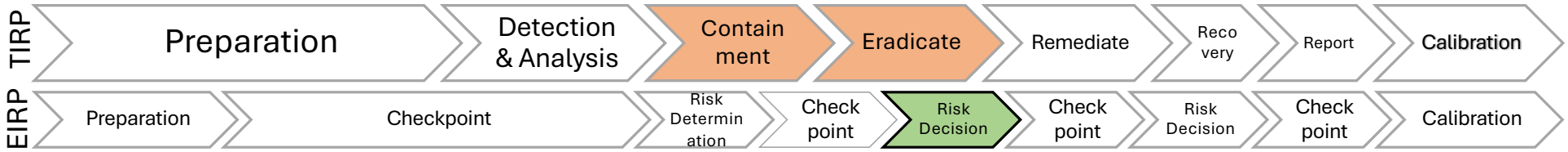

## Key Questions:

- What is the confirmed impact to operations and revenue?
- Are critical services or safety systems impaired?
- Do we have evidence of data exfiltration?
- What containment actions are proposed, and what are the business consequences?

## Key Deliverables:

- Agreed materiality level (operational, financial, reputational).
- Business Impact framing (functions disrupted, potential losses).
- Authorization to proceed with specific containment actions.
- Initial external notification and comms direction (internal, partners, regulators if required).

CyberFoundry



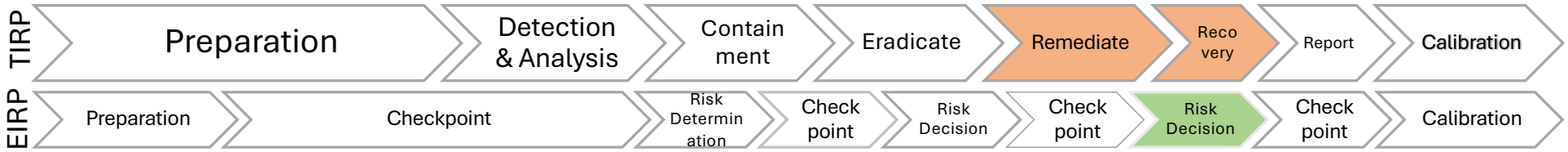

## Key Questions:

- Has containment stopped the spread?
- What are the options for eradication, and what are their business impacts?
- Do we accept the loss of evidence, downtime, or systems to ensure clean rebuilds?
- Are we paying a ransom or pursuing eradication independently?

## Key Deliverables:

- Executive validation that containment succeeded.
- Approval of eradication strategy (wipe, rebuild, credential resets).
- Formal ransom posture (default = no pay, exceptions documented).
- Evidence handling and law enforcement coordination direction.

CyberFoundry



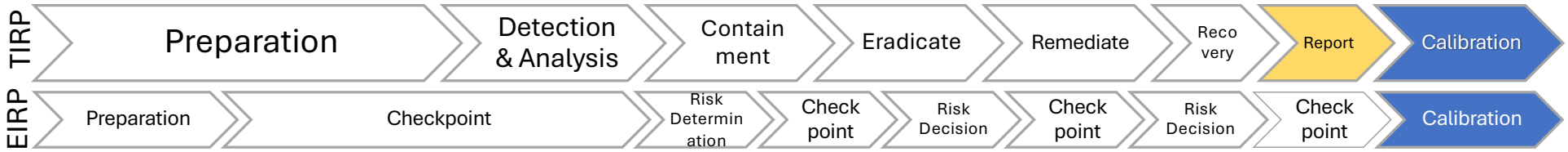

## Key Questions:

- Have remediation activities sufficiently reduced the threat?
- Which systems or business services should be prioritized for recovery?
- Are we willing to delay recovery of lower-priority systems to reduce risk?
- What level of residual risk are we accepting to resume operations?

## Key Deliverables:

- Executive validation that remediation is complete enough to proceed.
- Business-driven recovery priority list (tiered services).
- Authorization to initiate staged recovery.
- Communications plan for employees, customers, partners, and regulators about recovery status.

CyberFoundry



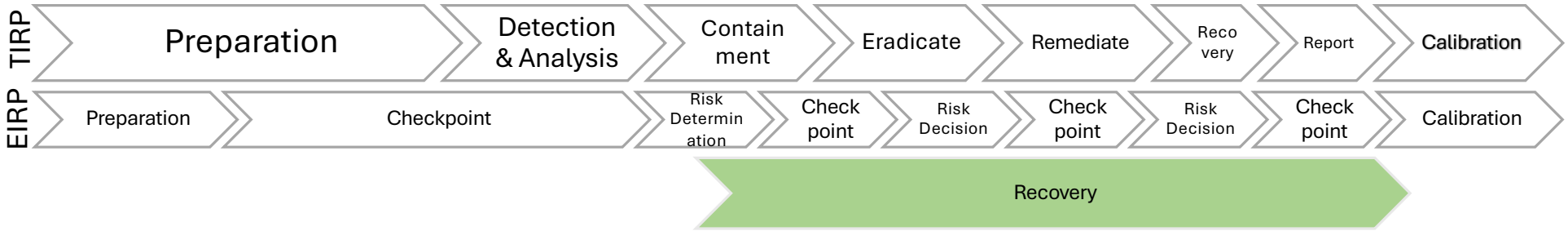

## Key Questions:

- What is the full narrative of the incident (timeline, actions, impact)?
- What do we communicate externally (board, regulators, customers, media) vs. keep internal under privilege?
- What lessons learned change our risk posture, BIA, or continuity plans?
- What investments or policy changes are needed to prevent recurrence?

## Key Deliverables:

- Final Incident Report from TIRP to EIRP (timeline, findings, actions).
- Privilege-protected executive report curated by General Counsel.
- Communications and regulatory filings approved (without breaching privilege).
- Updated BIA, IRP, and continuity policies.
- Executive decision log for board/regulators.

CyberFoundry




## Key Questions:

- What business, legal, and compliance losses were sustained (data, contracts, revenue)?
- Did sensitive data leave the environment (PII, PHI, ITAR, CUI, PCI)?
- What regulatory notifications or reporting obligations are triggered?
- What contractual or third-party partner obligations require disclosure or remediation?
- What remediation actions (technical or organizational) must be funded and tracked to closure?

## Key Deliverables:

- Loss assessment report: revenue, operations, contracts, data.
- Regulatory filing package: state/federal breach notifications, HIPAA, GDPR, SEC, DFARS/ITAR/CUI.
- Partner/customer communications aligned to contractual duties.
- Remediation roadmap: additional system hardening, data cleanup, audits.
- Executive decision log: acceptance of risk vs. remediation investment.

CyberFoundry

# What is a Tabletop Exercise

# A Good Tabletop Exercise...

Step-by-Step simulation of a cybersecurity incident with technical and leadership staff.

Tests the plan, roles and decision-making process.

Identifies gaps in process, communication, and coordination before a real event occurs.

This is not a Threat Hunting Exercise

# Tabletop Exercise

120 minutes at max.

Lets break for Lunch and then do one.

# agenda

**Part 1**
**Understanding the Incident Response Plan**

**Part 2**
**Tabletop Exercise**

## Pick Your Table

- We will assign roles
- No less than 5 people per table

CyberFoundry

# Part 2

Tabletop Exercise

**Join at slido.com**
**#3418410**

# Consolidated Nut & Bolt Company

”Just Screw It”

CyberFoundry

# Rules of Today's Tabletop Exercise

- We have created this tabletop to best reflect the threats to the organization.

  However, some creative liberates were taken.

- Please do not fight the narrative.
- Please be respectful of other members' responses.
- Disagreement is acceptable, but please see the previous bullet.

# Participation Is Encouraged

- This exercise won't succeed unless you each participate.
- When an inject relates to an area for which. You are responsible, please speak up.
- There are no write or wrong answers.
- Even if you are not responsible for the response to an inject, feel free to provide your opinion.

# Goals and Objectives

## Goal:

Conduct the organization's first ever tabletop exercise.

## Important:

Participants are not being graded or evaluated.

## Objectives:

- Build relationships within the team.
- Understand individual and team roles during a cybersecurity incident.
- Provide a written report of key areas for improvement.

# Consolidated Nut & Bolt Company

"Just Screw It"

Founded in 1954 in Gary, Indiana — family-owned turned global supplier
Specializes in **industrial fasteners**: screws, bolts, washers, and custom fittings
Plants across the Midwest serving automotive, aerospace, and heavy manufacturing
Known for **reliability, volume production, and down-to-earth culture**

Current challenge: aging infrastructure and outdated OT systems leave operations **vulnerable to cyber disruption**

CyberFoundry

# Choose Your Adventure

**CISO**
**Incident**
**Commander**

1 Person

**SOC**
**Incident**
**Response Team**

2+ People

**Information**
**Technology Tea**

2+ People

**Executive**
**Sponsor**

1 Person

**General**
**Council**

1 Person

CyberFoundry

# Reporting Out

CyberFoundry

# Friday 3:14 AM

TIRP

Preparation | Detection & Analysis | Contain | Eradicate | Remediate | Recover | Report | Calibration


## TIRP INJECT 1

Friday 3:14AM – IT Help Desk

Calls the CISO and says “The factory shut down about an hour ago. The computers all have this message on their screen. Something about being encrypted.

...so we called you.  Can you fix it?”

CyberFoundry

# Based on the known facts, would this be considered a cybersecurity incident?

TIRP

Preparation | Detection & Analysis | Contain | Eradicate | Remediate | Recover | Report | Calibration

## Key Activities

### Detection & Initial Triage

- Confirm the activity
- Escalate to the IRP

### Initial Containment

- Disconnect affected systems
- Identify what must keep running for safety

### Assessment

- Determine scope
- Stop additional damage (if possible)

## Key Questions

Scope & Impact

- Which business systems are impacted
- Is safety a concern

Detection

- What are our IOCs / SOIs?

Containment

- How do we isolate the problem?
- What is our plan for this?

Decision Making

- Do we have enough information to declare an incident?

CyberFoundry

**Did you decide to disconnect the company from the internet?**
**If so, who has that authority?**

# Friday 4:27 AM

TIRP

Preparation | Detection & Analysis | Contain | Eradicate | Remediate | Recover | Report | Calibration


## TIRP INJECT 2

Friday 4:27AM – War Room

IRT has identified the process that is running on the infected machines and why it wasn't detected earlier. They have what they believe to be an effective Indicator of Compromise (IOC) and have started scanning for it across the enterprise.

TOOLS:
EDR, SIEM

CyberFoundry

TIRP

Preparation | Detection & Analysis | Contain | Eradicate | Remediate | Recover | Report | Calibration

## Key Activities

### Detection & Initial Triage

- Confirm the activity
- Escalate to the IRP

### Initial Containment

- Disconnect affected systems
- Identify what must keep running for safety

### Assessment

- Determine scope
- Stop additional damage (if possible)

## Key Questions

Scope & Impact

- Which business systems are impacted
- Is safety a concern

Detection

- What are our IOCs / SOIs?

Containment

- How do we isolate the problem?
- What is our plan for this?

Decision Making

- Do we have enough information to declare an incident?

CyberFoundry

TIRP

Preparation | Detection & Analysis | Contain | Eradicate | Remediate | Recover | Report | Calibration

## Starting Gate

- Monitoring / logging active
- Incident criteria (classification matrix) ready

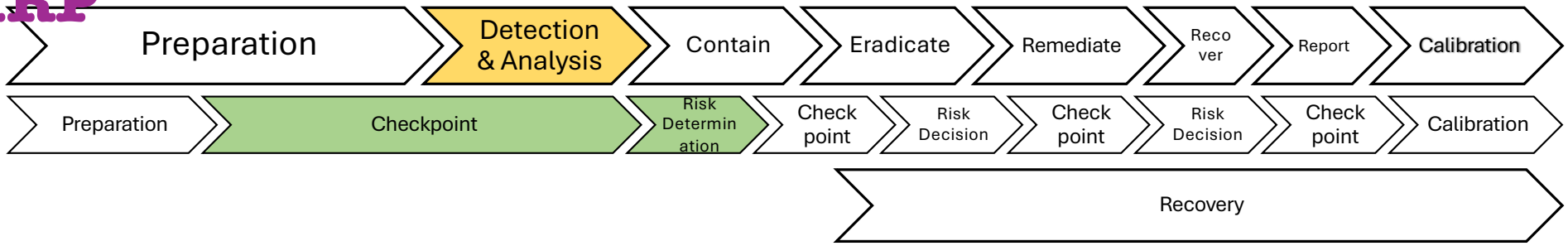
## Exit Gate

- Incident ticket created with initial classification
- Scope defined and validated
- Do we know enough to move into containment?

CyberFoundry

# Friday 8:00 AM

EIRP




## EIRP INJECT 1

Friday 8:00 EIRP War Room

Friday @ 3:57AM we declared a cybersecurity incident after notification from our users in the Gary IN factory that computers were inoperable.
We have found what we believe to be a ransomware infection affecting at least 14% of that site making the factory floor inoperable. We have taken initial triage steps to limit the damage. The IRT is responding and we expect to move into containment within the next 30 minutes.

CyberFoundry

EIRP

Preparation → Checkpoint → Risk Determination → Check point → Risk Decision → Check point → Risk Decision → Check point → Calibration

## Key Activities

| Business Operations | Mobilize | One Voice |
|---|---|---|
| • Discuss LOB impact<br>• Discover missing components of impact | • Coordinate within business<br>• Make resources available | • Respond to calls for action<br>• Share thinking on business impact |

## Key Questions:

Operational Impact

- Which critical business functions are down?
- How long can we sustain a shutdown?
- Do we need to activate our business continuity plan?

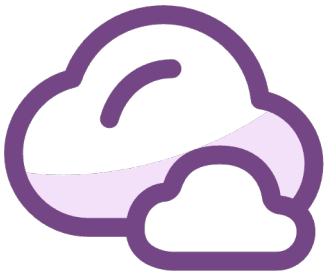
Safety &. Compliance

- Are there risks to employee safety?
- Are there regulatory obligations?
- Is protected data impacted?

Financial Exposure

- Cost of downtime per day?
- Do we have cyber insurance coverage? Who do we call?
- Are we at risk of breaching supplier / customer agreements?

CyberFoundry



**As the EIRP Executive Sponsor, you're responsible for mitigating the impact to the business. Who are some of the people you would be calling?**

EIRP

Preparation | Checkpoint | Risk Determination | Check point | Risk Decision | Check point | Risk Decision | Check point | Calibration

## Executive Sponsor

- Who did you call?
- What did you share?
- How does this impact your strategy?

CyberFoundry

# Friday 9:27 AM

TIRP

Preparation | Detection & Analysis | Contain | Eradicate | Remediate | Recover | Report | Calibration

## TIRP INJECT 3

Friday 9:27AM – War Room

The IRT reports that they are able to remove the malware now that their tools can see it, but the IT Help Desk keeps opening new tickets for infected machines.

CyberFoundry

# What would your next step be?

TIRP

Preparation | Detection & Analysis | Contain | Eradicate | Remediate | Recover | Report | Calibration

## How ya doing Incident Commander?

- Are you confident in your containment strategy?
- What did you communicate to your EIRP team?

CyberFoundry

# Friday 12:15 PM

TIRP

Preparation | Detection & Analysis | Contain | **Eradicate** | Remediate | Recover | Report | Calibration

## TIRP INJECT 4

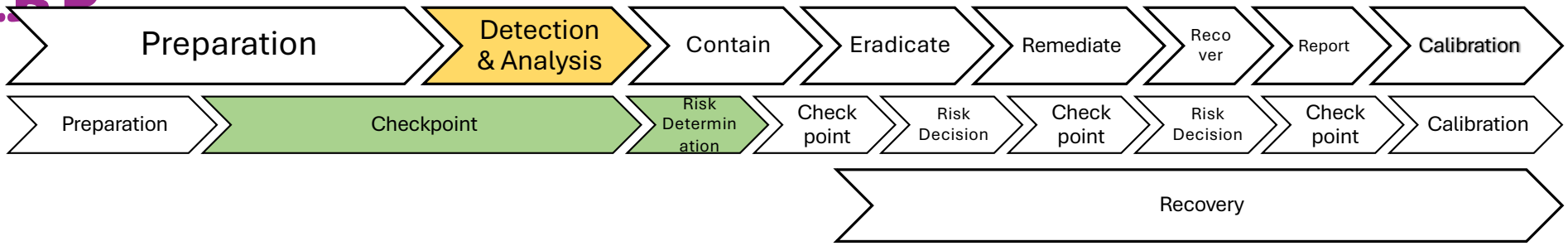
Friday 12:15PM – War Room

The IT Team has started reclaiming infected systems. The Network Team reports that there is an exceptional amount of traffic leaving the network for the internet and asks if you can cutback on whatever you're doing to give them a break.

CyberFoundry

# What do you do next?

EIRP



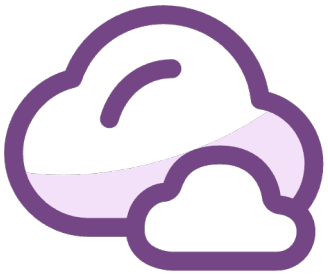

## EIRP INJECT 2

Friday 12:37PM – Your Desk

Your Executive Sponsor introduces you to the Forensic Analyst and Breach Coach the Insurance Company has retained to help you.

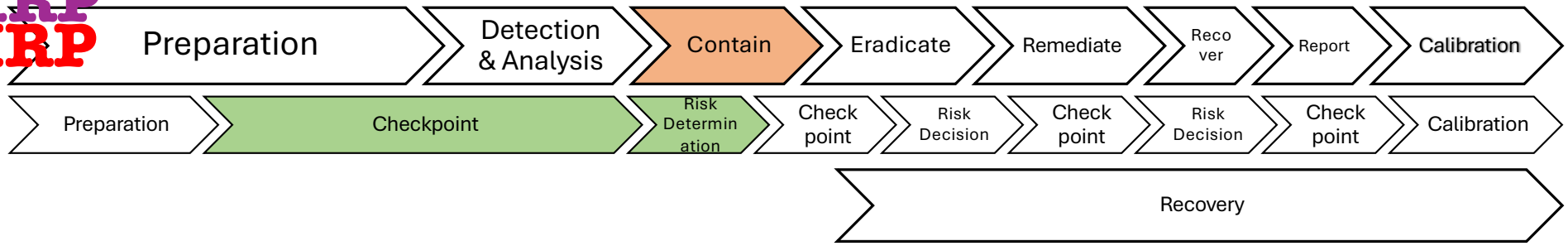
They would like access to all of your work and will be reporting to the General Council.

CyberFoundry



# What does this mean?

EIRP
TIRP




## How ya doing Incident Commander?

- Are you confident in your eradication strategy?
- What did you communicate to your EIRP team?
- How did you handle the Forensic Analyst from the Insurance Company?

CyberFoundry

# Friday 3:21 PM

TIRP

Preparation | Detection & Analysis | Contain | Eradicate | **Remediate** | Recover | Report | Calibration

## TIRP INJECT 5

Friday 3:21PM – War Room

The SOC found an outdated version of Java running on many of the infected machines and believe it may be the cause of the ransomware's spread across the environment. This is new information.

IT tells you that the specific version of Java they are using is a hard requirement for the ERP system and that updating it will break the business.

CyberFoundry

# What are your options?

EIRP

Preparation | Checkpoint | Risk Determination | Check point | Risk Decision | Check point | Risk Decision | Check point | Calibration

## EIRP INJECT 3

Friday 4:12PM – Your Desk

Your General Council reminds you that the company has 48 hours to report any material losses to the SEC, and even less time to call your customer if there was a material breach of your protected information.

The network team analysis shows that significant information was exfiltrated over the last 48 hours.

CyberFoundry

# Is this a material impact?

# What information do you. need to start getting ready now for your general council?

TIRP

Preparation | Detection & Analysis | Contain | Eradicate | **Remediate** | Recover | Report | Calibration

## How ya doing Incident Commander?

- Are you confident that the outdated software is the source of the problem?
- What information do you report to the EIRP? What decisions to you ask them to consider?
- Do you have any alternatives?

CyberFoundry

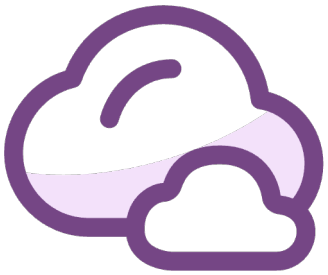
TIRP
EIRP

Preparation | Detection & Analysis | Contain | Eradicate | Remediate | Recover | Report | Calibration

Preparation | Checkpoint | Risk Determination | Check point | Risk Decision | Check point | Risk Decision | Check point | Calibration

Its three months later, and a lot of long meetings with staff and your leadership team.

CyberFoundry



# What did you learn?

# Thank you for participating.


This story brought to you by CVE-2008-5353, CVE-2009-1103, CVE-2010-0840, CVE-2011-3544, CVE-2012-4681, CVE-2013-2465, CVE-2014-2490, CVE-2015-2590, CVE-2016-3427, CVE-2017-10086, CVE-2018-3183, CVE-2019-2698, CVE-2020-14664, CVE-2021-44228, CVE-2022-22965, CVE-2023-46606, CVE-2023-46364.

CyberFoundry

# Let’s Do This Again…

We can deliver a tailored Incident Response Plan
and Tabletop for your company.


https://www.cyberfoundry.io/bsides-resources/