Grimlin

After-Action Report

Operation Iron Horizon · July 22, 2026

EXECUTIVE SUMMARY

This exercise ran the "Operation Iron Horizon" scenario (Ransomware / Double Extortion), concluding with an overall result of "Contained, But Costly." The team's strongest area was Containment Effectiveness, scoring 8 out of 10. The most significant gap identified was Business Continuity, scoring 4 out of 10 - the highest-priority focus area for remediation. Data exposure was confirmed during this exercise, elevating the urgency of the associated improvement actions.

EXERCISE OVERVIEW

Scenario	Operation Iron Horizon
Threat Type	Ransomware / Double Extortion
Setting	Global manufacturing conglomerate, ~340 sites, 40 countries, OT/IT-converged plants
Format	Multiplayer (team)
Date	July 22, 2026
Duration	57 minutes
Participants	Morgan Ellis (Chief Information Security Officer), Priya Natarajan (SOC Incident Commander), Elena Kowalski (Chief Compliance Officer), Devon Osei (VP of Infrastructure & Recovery)

Objectives

- Contain the ransomware's lateral spread across OT/IT boundaries before it reaches a second site.
- Coordinate executive, legal, and technical response without losing stakeholder trust.
- Determine appropriate regulatory disclosure timing under SEC and multi-jurisdiction requirements.
- Restore operations securely without reintroducing the same architectural exposure.

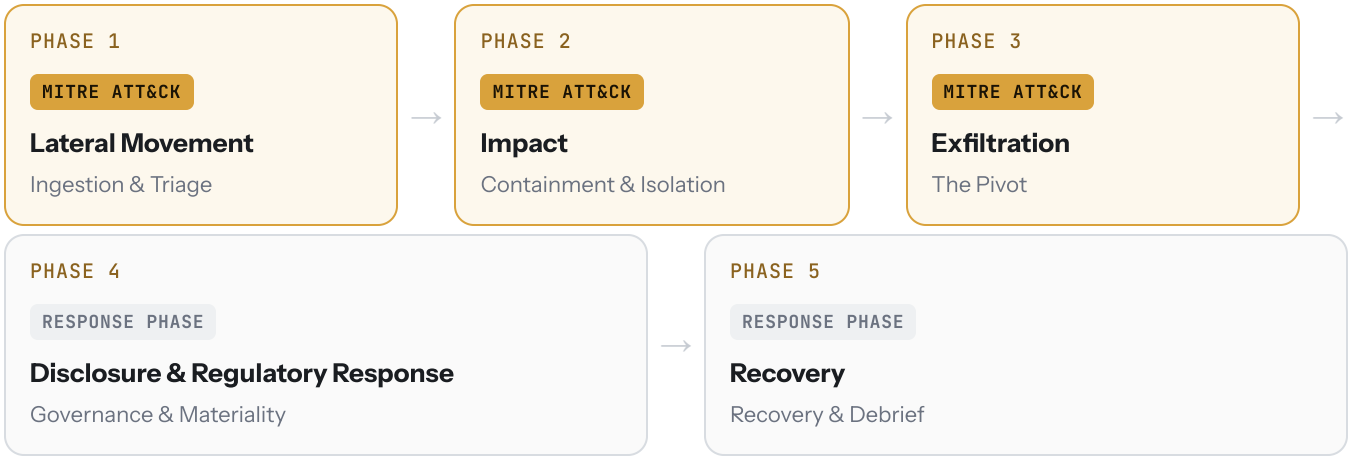
SCENARIO SUMMARY

Ransomware has hit the production network of a major manufacturing plant, causing physical safety shutdown loops and threatening lateral propagation to adjacent sites.

- **Phase 1 - Ingestion & Triage:** Initial ransomware detection and the first command decisions on isolation versus visibility.
- **Phase 2 - Containment & Isolation:** Operations grind to a halt as the team weighs transparency, the ransom demand, and recovery method.
- **Phase 3 - The Pivot:** A complication emerges based on how well containment held, forcing a response to escalating exposure.
- **Phase 4 - Governance & Materiality:** Board, regulatory, and technical decisions on disclosure timing and resumption of operations.
- **Phase 5 - Recovery & Debrief:** The final outcome resolves from the accumulated state of the response across the first four phases.

MITRE ATT&CK ALIGNMENT

This exercise's five phases, mapped against real attacker tactics from the MITRE ATT&CK® Enterprise framework where the phase reflects an actual attacker technique - phases that are purely governance or recovery are labeled as such rather than forced into a tactic that doesn't really apply.



TIMELINE OF DECISIONS

PHASE 1 - INGESTION & TRIAGE • CHIEF INFORMATION SECURITY OFFICER

How do you coordinate the initial command response?

Decision: Declare a P1 corporate incident immediately, spin up the crisis bridge, and notify executive leadership.

Outcome: Leadership is engaged early, but panic spreads across departments.

PHASE 1 - INGESTION & TRIAGE • CHIEF INFORMATION SECURITY OFFICER

Who do you personally notify before the crisis bridge even convenes?

Decision: Call the Board Chair and General Counsel directly, before the scope is even confirmed.

Outcome: Leadership has no surprises later, but you're now fielding board questions before you have real answers.

PHASE 1 - INGESTION & TRIAGE • SOC INCIDENT COMMANDER

Where do you focus your forensic triage?

Decision: Run automated EDR endpoint isolation scripts on all active hosts in the Frankfurt subnet immediately.

Outcome: You slow down the attacker, but shut down several plant management consoles.

PHASE 1 - INGESTION & TRIAGE • SOC INCIDENT COMMANDER

What do you do with the suspected patient-zero engineering workstation?

Decision: Pull it off the network immediately, accepting the loss of any memory-resident evidence.

Outcome: You cut off a confirmed entry point fast, but the forensic picture of exactly how it was compromised stays incomplete.

PHASE 1 - INGESTION & TRIAGE • CHIEF COMPLIANCE OFFICER

How do you baseline the compliance impact?

Decision: Instruct legal to document all initial logs under attorney-client privilege and review contractual SLA liabilities with customers.

Outcome: Your legal position is secured, but operational departments feel the overhead.

PHASE 1 - INGESTION & TRIAGE • CHIEF COMPLIANCE OFFICER

Do you engage outside breach counsel at this early stage?

Decision: Engage outside counsel now, establishing privilege over the investigation from the start.

Outcome: Your investigation record is protected, but outside counsel's process adds friction to every early decision.

PHASE 1 - INGESTION & TRIAGE • VP OF INFRASTRUCTURE & RECOVERY

What is your immediate network action?

Decision: Sever the site-to-site VPN connection between Frankfurt and the corporate WAN immediately.

Outcome: The infection is isolated to Frankfurt, but all remote telemetry and monitoring are severed.

PHASE 1 - INGESTION & TRIAGE • VP OF INFRASTRUCTURE & RECOVERY

How do you handle the OT/IT boundary firewall's logs before making further changes?

Decision: Export and back up the boundary firewall logs first, before any further configuration changes.

Outcome: You preserve a clean record of exactly how the boundary was crossed, but lose a few minutes of response time.

PHASE 2 - CONTAINMENT & ISOLATION • CHIEF INFORMATION SECURITY OFFICER

How do you manage the pressure to resume operations?

Decision: Release a transparent statement acknowledging a cybersecurity incident and confirming containment is underway.

Outcome: Transparency builds long-term trust, but triggers immediate inquiry from regulators.

PHASE 2 - CONTAINMENT & ISOLATION • CHIEF INFORMATION SECURITY OFFICER

The CEO wants an hourly cost figure to give the board. Do you provide one?

Decision: Provide a conservative, defensible per-hour figure now, caveated as preliminary.

Outcome: The board gets a number to act on, but it will need revising as the picture changes, inviting scrutiny.

PHASE 2 - CONTAINMENT & ISOLATION • CHIEF INFORMATION SECURITY OFFICER

URGENT — A journalist just emailed asking to confirm reports of a ransomware attack on your Frankfurt facility. You have minutes before they publish with or without a comment.

Decision: Provide a brief, honest 'we are investigating a cybersecurity incident' holding statement immediately.

Outcome: The quote is measured, but it confirms the story is real before you've told the board yourselves.

PHASE 2 - CONTAINMENT & ISOLATION • SOC INCIDENT COMMANDER

How do you contain the threat actor's active session?

Decision: Trigger a global password reset for all administrative credentials and revoke active OAuth tokens.

Outcome: Active sessions are severed, but support engineers are locked out of critical recovery tools.

PHASE 2 - CONTAINMENT & ISOLATION • SOC INCIDENT COMMANDER

The dual-homed engineering laptop's NIC bypassed the Purdue boundary. Do you audit for other dual-homed devices now?

Decision: Immediately sweep the entire OT network for any other dual-homed or bridging devices.

Outcome: You may catch other hidden bypass points, but the sweep itself disrupts several in-progress recovery tasks.

PHASE 2 - CONTAINMENT & ISOLATION • SOC INCIDENT COMMANDER

URGENT — A reporter's inquiry just hit the corporate press inbox, cc'ing your director. Someone outside your team is now asking pointed technical questions about scope.

Decision: Route all technical questions to the executive team and refuse to speak to press directly, sticking to your incident work.

Outcome: You stay focused on the actual incident, and press handling stays where it belongs.

PHASE 2 - CONTAINMENT & ISOLATION • CHIEF COMPLIANCE OFFICER

What is your recommendation regarding the ransom demand?

Decision: Formally advise against any negotiation, noting OFAC sanctions risk if the threat actor is a designated entity.

Outcome: You comply with federal guidance, but face extended operational downtime.

PHASE 2 - CONTAINMENT & ISOLATION • CHIEF COMPLIANCE OFFICER

Do you notify cyber insurance at this stage?

Decision: Notify the cyber insurance carrier immediately, even before the ransom question is resolved.

Outcome: Coverage and incident-response resources become available faster, but the carrier's own requirements now shape your options.

PHASE 2 - CONTAINMENT & ISOLATION • CHIEF COMPLIANCE OFFICER

URGENT — Press is asking questions before any regulatory notification has gone out. If this story breaks first, regulators may treat the leak as your de facto disclosure.

Decision: Advise executive leadership to issue a brief factual statement now, framing it as the source of record ahead of the story.

Outcome: Getting ahead of the story on your own terms strengthens your regulatory position — you defined the narrative instead of reacting to someone else's.

PHASE 2 - CONTAINMENT & ISOLATION • VP OF INFRASTRUCTURE & RECOVERY

How do you secure a path to recovery?

Decision: Isolate a clean environment in the cloud and begin pulling offsite offline tape backups for restoration.

Outcome: Backups are verified clean, but the restoration process will take days.

PHASE 2 - CONTAINMENT & ISOLATION • VP OF INFRASTRUCTURE & RECOVERY

The wiped NAS share held the local backups. Do you investigate how the attacker got write access to it?

Decision: Dedicate a team to trace exactly how the attacker reached and wiped the NAS share before rebuilding it.

Outcome: You learn precisely how backups were destroyed, but rebuilding the backup target itself is delayed.

PHASE 2 - CONTAINMENT & ISOLATION • VP OF INFRASTRUCTURE & RECOVERY

URGENT — IT support is fielding a spike of calls: internal staff are asking if their own laptops are safe to use right now.

Decision: Send a brief, calm all-staff notice confirming the affected scope and that most systems are unaffected.

Outcome: Panic subsides, but drafting and clearing the notice pulls you off the technical work for a bit.

PHASE 3 - THE PIVOT • CHIEF INFORMATION SECURITY OFFICER

Do you authorize negotiations to buy time?

Decision: Authorize the negotiator to offer a token payment to delay the leak site countdown.

Outcome: You buy 48 hours, but leak site snippets expose sensitive data to competitors.

PHASE 3 - THE PIVOT • CHIEF INFORMATION SECURITY OFFICER

The attackers threaten to also email the leaked CAD drawings directly to your top competitors. How do you respond?

Decision: Get ahead of it: notify those competitors' legal teams yourself that stolen material may reach them.

Outcome: You establish a clean paper trail against future misuse claims, but effectively confirm the breach to rivals yourself.

PHASE 3 - THE PIVOT • CHIEF INFORMATION SECURITY OFFICER

URGENT — The leak site's public countdown clock reads 00:02:00 and falling. A reporter is on hold demanding comment before it hits zero.

Decision: Get on the record immediately: confirm the incident is real and that a fuller statement is coming shortly.

Outcome: The quick, honest acknowledgment reads as competent under pressure, but you've now confirmed the incident publicly before legal or GRC signed off on any language.

PHASE 3 - THE PIVOT • SOC INCIDENT COMMANDER

Where do you redirect your hunting team?

Decision: Deploy active honeytokens and file integrity monitoring across all uncompromised plants to watch for lateral pivots.

Outcome: You secure adjacent plants, but local forensic analysis on Frankfurt patient zero is delayed.

PHASE 3 - THE PIVOT • SOC INCIDENT COMMANDER

Do you attribute the attack to a specific known ransomware group?

Decision: Commit to a formal attribution now, based on the payload's code overlap with a known group.

Outcome: Leadership gets a concrete adversary to plan around, but a wrong attribution would undermine the whole response.

PHASE 3 - THE PIVOT • CHIEF COMPLIANCE OFFICER

What is your disclosure recommendation to the Board?

Decision: Recommend filing an SEC Form 8-K immediately to report a material cyber incident, publicizing the breach.

Outcome: Full compliance is achieved, but stock price faces immediate short-term volatility.

PHASE 3 - THE PIVOT • CHIEF COMPLIANCE OFFICER

GDPR's 72-hour clock is running on the EU customer data in the exfiltrated files. Do you file now or wait for full scope?

Decision: File the GDPR notification now with the scope known so far, planning to supplement it later.

Outcome: You meet the 72-hour deadline cleanly, but the supplemental filing later draws its own scrutiny.

PHASE 3 - THE PIVOT • VP OF INFRASTRUCTURE & RECOVERY

How do you handle the Active Directory recovery?

Decision: Execute a Forest Recovery, rebuilding the AD forest from clean offline system state backups.

Outcome: You restore identity services, but must manually rotate all trust passwords.

PHASE 3 - THE PIVOT • VP OF INFRASTRUCTURE & RECOVERY

Do you rebuild Chicago's domain controllers now too, or only Frankfurt's?

Decision: Focus entirely on Frankfurt first and only touch Chicago if evidence of compromise actually appears.

Outcome: Frankfurt recovers faster with full attention, but Chicago's domain controllers remain an open question.

PHASE 4 - GOVERNANCE & MATERIALITY • CHIEF INFORMATION SECURITY OFFICER

How do you present the incident report to the Board?

Decision: Present a conservative recovery timeline focusing on long-term architecture hardening, prioritizing security.

Outcome: The board supports the security upgrades, but operations departments complain of low speed.

PHASE 4 - GOVERNANCE & MATERIALITY • CHIEF INFORMATION SECURITY OFFICER

The board asks whether anyone should be held personally accountable. How do you respond?

Decision: Commission an independent, blameless post-incident review focused on process gaps, not individuals.

Outcome: The team trusts future reporting more, but some board members feel accountability was dodged.

PHASE 4 - GOVERNANCE & MATERIALITY • CHIEF INFORMATION SECURITY OFFICER

The board wants one unified public position before the press conference in an hour: how much does the company say, right now, about what happened and what's being done about it?

Decision: Confirmed-facts-only: acknowledge the incident and confirmed exposure, but withhold technical/architectural detail as 'an ongoing security matter.'

Outcome: A balanced, defensible position that satisfies immediate disclosure obligations without handing out a blueprint — though some press and analysts push back on the vagueness around what's actually being fixed.

PHASE 4 - GOVERNANCE & MATERIALITY • SOC INCIDENT COMMANDER

How do you share threat intelligence?

Decision: Share the extracted indicators of compromise (IOCs) with ISAC and CISA to protect other manufacturing plants.

Outcome: You are recognized for leadership, and national defense is strengthened.

PHASE 4 - GOVERNANCE & MATERIALITY • SOC INCIDENT COMMANDER

Do you recommend a full red-team validation of the rebuilt environment before declaring recovery complete?

Decision: Insist on a red-team validation pass before signing off, even though it delays the formal all-clear.

Outcome: You catch any remaining gaps before they matter, but the formal 'all clear' slips by several more days.

PHASE 4 - GOVERNANCE & MATERIALITY • CHIEF COMPLIANCE OFFICER

How do you handle notifications to affected customers?

Decision: Send detailed notifications to all affected customers containing forensic details of the exfiltrated data files.

Outcome: You satisfy compliance requirements, but deal with customer support spikes.

PHASE 4 - GOVERNANCE & MATERIALITY • CHIEF COMPLIANCE OFFICER

Do you offer affected customers credit monitoring or a similar remediation service?

Decision: Proactively offer credit monitoring and identity protection to every affected customer, unprompted.

Outcome: Customer goodwill is preserved, but the ongoing service cost lands on this quarter's budget.

PHASE 4 - GOVERNANCE & MATERIALITY • VP OF INFRASTRUCTURE & RECOVERY

How do you execute the plant boot sequence?

Decision: Verify and bind all local systems to the new isolated subnet, routing all OT traffic through inspection firewalls.

Outcome: The plant resumes securely, but legacy machinery experiences minor communication latency.

PHASE 4 - GOVERNANCE & MATERIALITY • VP OF INFRASTRUCTURE & RECOVERY

Do you roll the same OT/IT segmentation fix out to the other 339 plants now, or just Frankfurt?

Decision: Fund and schedule the segmentation fix across every plant immediately, using this incident as justification.

Outcome: The same exposure is closed company-wide, but the rollout strains engineering resources for months.

PERFORMANCE ASSESSMENT

Containment Effectiveness	8/10
Stakeholder Communication	7/10
Regulatory Posture	8/10
Business Continuity	4/10
Data Exposure	Confirmed

OBSERVATIONS

Strengths

- Containment Effectiveness performed well (8/10), reflecting effective decisions across the exercise.
- Stakeholder Communication performed well (7/10), reflecting effective decisions across the exercise.
- Regulatory Posture performed well (8/10), reflecting effective decisions across the exercise.

Areas of Concern

- Business Continuity scored 4/10, indicating an area for focused improvement.

IMPROVEMENT PLAN

IDENTIFIED GAP	RECOMMENDED TRAINING MODULE	RATIONALE	OWNER	TARGET DATE
Platform Resilience & Recovery	Platform & Cloud Security	Recovery and continuity took longer or cost more than it needed to — infrastructure resilience planning would help here.		
Data Loss Prevention	Data Governance & Loss Prevention	Sensitive data was confirmed exfiltrated during this run — stronger data protection controls could have prevented or limited this.		

FRAMEWORK ALIGNMENT

Performance metrics in this report map to the following NIST Cybersecurity Framework (CSF) 2.0 functions:

METRIC	NIST CSF 2.0 FUNCTION
Containment Effectiveness	Respond
Stakeholder Communication	Respond / Communications
Regulatory Posture	Govern
Business Continuity	Recover
Data Exposure	Protect / Detect

APPENDIX: FULL DECISION LOG

PHASE	ROLE	DECISION	STATE DELTAS
Phase 1	Chief Information Security Officer	Declare a P1 corporate incident immediately, spin up the crisis bridge, and notify executive leadership.	stakeholderTrust: +1, containmentSpeed: +1
Phase 1	Chief Information Security Officer	Call the Board Chair and General Counsel directly, before the scope is even confirmed.	stakeholderTrust: +1, regulatoryStanding: +1
Phase 1	SOC Incident Commander	Run automated EDR endpoint isolation scripts on all active hosts in the Frankfurt subnet immediately.	containmentSpeed: +2, businessContinuity: -1
Phase 1	SOC Incident Commander	Pull it off the network immediately, accepting the loss of any memory-resident evidence.	containmentSpeed: +1, stakeholderTrust: -1
Phase 1	Chief Compliance Officer	Instruct legal to document all initial logs under attorney-client privilege and review contractual SLA liabilities with customers.	regulatoryStanding: +1
Phase 1	Chief Compliance Officer	Engage outside counsel now, establishing privilege over the investigation from the start.	regulatoryStanding: +1, stakeholderTrust: -1
Phase 1	VP of Infrastructure & Recovery	Sever the site-to-site VPN connection between Frankfurt and the corporate WAN immediately.	containmentSpeed: +2, businessContinuity: -2
Phase 1	VP of Infrastructure & Recovery	Export and back up the boundary firewall logs first, before any further configuration changes.	businessContinuity: -1, stakeholderTrust: +1
Phase 2	Chief Information Security Officer	Release a transparent statement acknowledging a cybersecurity incident and confirming containment is underway.	stakeholderTrust: +2, regulatoryStanding: -1
Phase 2	Chief Information Security Officer	Provide a conservative, defensible per-hour figure now, caveated as preliminary.	stakeholderTrust: +1, regulatoryStanding: -1
Phase 2	Chief Information Security Officer	Provide a brief, honest 'we are investigating a cybersecurity incident' holding statement immediately.	stakeholderTrust: +1, regulatoryStanding: -1
Phase 2	SOC Incident Commander	Trigger a global password reset for all administrative credentials and revoke active OAuth tokens.	containmentSpeed: +2, businessContinuity: -1
Phase 2	SOC Incident Commander	Immediately sweep the entire OT network for any other dual-homed or bridging devices.	containmentSpeed: +1, businessContinuity: -1
Phase 2	SOC Incident Commander	Route all technical questions to the executive team and refuse to speak to press directly, sticking to your incident work.	containmentSpeed: +1

PHASE	ROLE	DECISION	STATE DELTAS
Phase 2	Chief Compliance Officer	Formally advise against any negotiation, noting OFAC sanctions risk if the threat actor is a designated entity.	regulatoryStanding: +2, businessContinuity: -1
Phase 2	Chief Compliance Officer	Notify the cyber insurance carrier immediately, even before the ransom question is resolved.	regulatoryStanding: +1, businessContinuity: +1
Phase 2	Chief Compliance Officer	Advise executive leadership to issue a brief factual statement now, framing it as the source of record ahead of the story.	regulatoryStanding: +1, stakeholderTrust: +1
Phase 2	VP of Infrastructure & Recovery	Isolate a clean environment in the cloud and begin pulling offsite offline tape backups for restoration.	containmentSpeed: +1, businessContinuity: +1
Phase 2	VP of Infrastructure & Recovery	Dedicate a team to trace exactly how the attacker reached and wiped the NAS share before rebuilding it.	businessContinuity: -1, containmentSpeed: +1
Phase 2	VP of Infrastructure & Recovery	Send a brief, calm all-staff notice confirming the affected scope and that most systems are unaffected.	stakeholderTrust: +1, containmentSpeed: -1
Phase 3	Chief Information Security Officer	Authorize the negotiator to offer a token payment to delay the leak site countdown.	stakeholderTrust: -1, dataExposureConfirmed: true
Phase 3	Chief Information Security Officer	Get ahead of it: notify those competitors' legal teams yourself that stolen material may reach them.	stakeholderTrust: +1, regulatoryStanding: -1
Phase 3	Chief Information Security Officer	Get on the record immediately: confirm the incident is real and that a fuller statement is coming shortly.	stakeholderTrust: +1, regulatoryStanding: -1
Phase 3	SOC Incident Commander	Deploy active honeytokens and file integrity monitoring across all uncompromised plants to watch for lateral pivots.	containmentSpeed: +2
Phase 3	SOC Incident Commander	Commit to a formal attribution now, based on the payload's code overlap with a known group.	stakeholderTrust: +1, containmentSpeed: -1
Phase 3	Chief Compliance Officer	Recommend filing an SEC Form 8-K immediately to report a material cyber incident, publicizing the breach.	regulatoryStanding: +2, stakeholderTrust: -1
Phase 3	Chief Compliance Officer	File the GDPR notification now with the scope known so far, planning to supplement it later.	regulatoryStanding: +2
Phase 3	VP of Infrastructure & Recovery	Execute a Forest Recovery, rebuilding the AD forest from clean offline system state backups.	containmentSpeed: +1, businessContinuity: -1

PHASE	ROLE	DECISION	STATE DELTAS
Phase 3	VP of Infrastructure & Recovery	Focus entirely on Frankfurt first and only touch Chicago if evidence of compromise actually appears.	containmentSpeed: -1, businessContinuity: +1
Phase 4	Chief Information Security Officer	Present a conservative recovery timeline focusing on long-term architecture hardening, prioritizing security.	stakeholderTrust: +2, businessContinuity: -1
Phase 4	Chief Information Security Officer	Commission an independent, blameless post-incident review focused on process gaps, not individuals.	stakeholderTrust: +2
Phase 4	Chief Information Security Officer	Confirmed-facts-only: acknowledge the incident and confirmed exposure, but withhold technical/architectural detail as 'an ongoing security matter.'	stakeholderTrust: +1, regulatoryStanding: +1
Phase 4	SOC Incident Commander	Share the extracted indicators of compromise (IOCs) with ISAC and CISA to protect other manufacturing plants.	regulatoryStanding: +2
Phase 4	SOC Incident Commander	Insist on a red-team validation pass before signing off, even though it delays the formal all-clear.	containmentSpeed: +1, businessContinuity: -1
Phase 4	Chief Compliance Officer	Send detailed notifications to all affected customers containing forensic details of the exfiltrated data files.	regulatoryStanding: +2, stakeholderTrust: +1
Phase 4	Chief Compliance Officer	Proactively offer credit monitoring and identity protection to every affected customer, unprompted.	stakeholderTrust: +2, businessContinuity: -1
Phase 4	VP of Infrastructure & Recovery	Verify and bind all local systems to the new isolated subnet, routing all OT traffic through inspection firewalls.	containmentSpeed: +2, businessContinuity: -1
Phase 4	VP of Infrastructure & Recovery	Fund and schedule the segmentation fix across every plant immediately, using this incident as justification.	containmentSpeed: +2, businessContinuity: -1