Zamlom

After-Action Report

Operation Iron Horizon · August 9, 2026

EXECUTIVE SUMMARY

This exercise ran the "Operation Iron Horizon" scenario (Ransomware / Double Extortion), concluding with an overall result of "Textbook Response." The team's strongest area was Containment Effectiveness, scoring 7 out of 10. The most significant gap identified was Stakeholder Communication, scoring 4 out of 10 - the highest-priority focus area for remediation. No data exposure was confirmed during this exercise.

EXERCISE OVERVIEW

Scenario	Operation Iron Horizon
Threat Type	Ransomware / Double Extortion
Setting	Global manufacturing conglomerate, ~340 sites, 40 countries, OT/IT-converged plants
Format	Solo
Date	August 9, 2026
Duration	25 minutes
Participants	Jordan Alvarez (Chief Information Security Officer)

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.

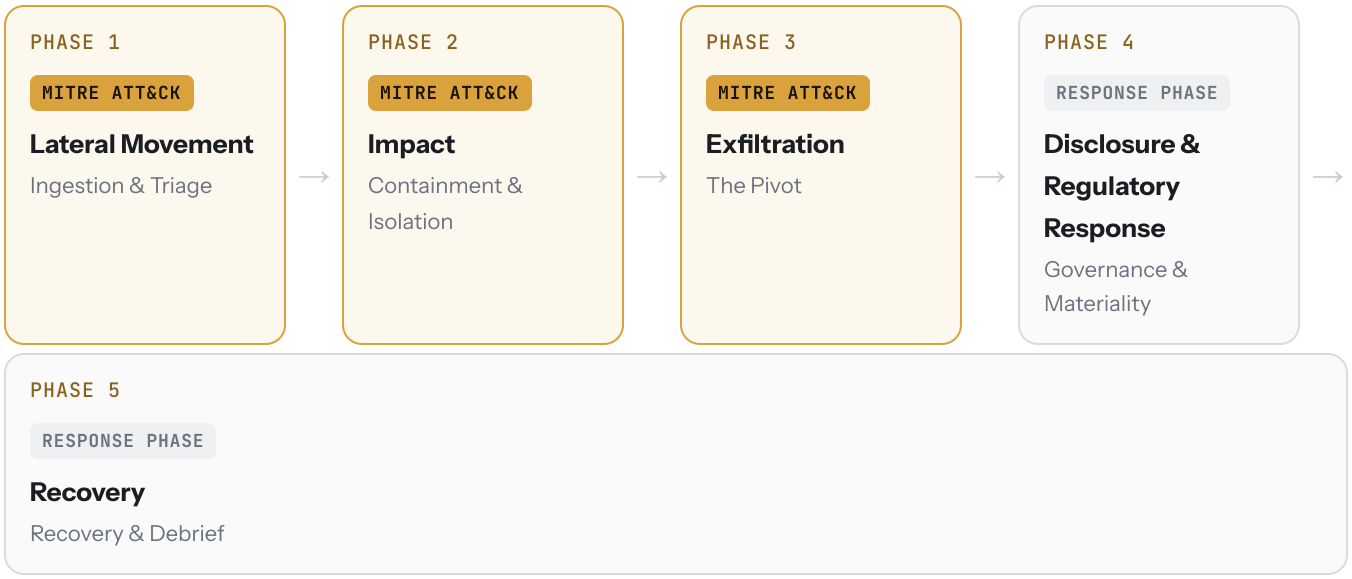
SCENARIO SUMMARY

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 +24M 37S

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.

`+1 Stakeholder Communication` `+1 Containment Effectiveness`

PHASE 1 - INGESTION & TRIAGE • CHIEF INFORMATION SECURITY OFFICER +0S

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

Decision: Wait for SOC's preliminary scope assessment before looping in anyone outside the crisis bridge.

Outcome: Your team can focus without interruption, but the board later feels they were told last.

`+1 Containment Effectiveness` `-1 Stakeholder Communication`

PHASE 2 - CONTAINMENT & ISOLATION • CHIEF INFORMATION SECURITY OFFICER +0S

How do you manage the pressure to resume operations?

Decision: Say nothing publicly and just quietly work the phones with your biggest customers one-on-one.

Outcome: Your biggest accounts feel personally reassured, but the version of events reaching everyone else is now a rumor, not your statement - and it's less flattering than the truth.

`-1 Stakeholder Communication` `+1 Business Continuity`

PHASE 2 - CONTAINMENT & ISOLATION • CHIEF INFORMATION SECURITY OFFICER +0S

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

Decision: Decline to estimate until finance can produce a verified figure, even if the board pushes back.

Outcome: Your eventual number holds up, but the board feels stonewalled during the wait.

`+1 Regulatory Posture` `-1 Stakeholder Communication`

PHASE 2 - CONTAINMENT & ISOLATION • CHIEF INFORMATION SECURITY OFFICER +0S

URGENT — Your phone lights up: a journalist from a trade publication 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.

`+1 Stakeholder Communication` `-1 Regulatory Posture`

PHASE 3 - THE PIVOT • CHIEF INFORMATION SECURITY OFFICER +0S

Do you authorize negotiations to buy time?

Decision: Refuse negotiation entirely, and direct the recovery team to focus solely on backup restoration.

Outcome: You maintain operational integrity, but the attackers publish the blueprints immediately.

`+1 Stakeholder Communication` `-1 Business Continuity`

PHASE 3 - THE PIVOT • CHIEF INFORMATION SECURITY OFFICER +0S

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

Decision: Contact the competitors' business leadership informally, framed as a professional courtesy heads-up.

Outcome: The gesture is well-intentioned, but without legal's involvement, two competitors discussing product IP informally becomes its own antitrust-adjacent question your own counsel has to untangle.

`-1 Stakeholder Communication` `-1 Regulatory Posture`

PHASE 3 - THE PIVOT • CHIEF INFORMATION SECURITY OFFICER +0S

URGENT — The leak site's public countdown clock reads 00:02:00 and falling on the mirror your comms team has up on the wall. A reporter is on hold demanding comment before it hits zero and the full CAD file set posts automatically.

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.

`+1 Stakeholder Communication` `-1 Regulatory Posture`

PHASE 4 - GOVERNANCE & MATERIALITY • CHIEF INFORMATION SECURITY OFFICER +0S

How do you present the incident report to the Board?

Decision: Commit to a fast resume-work date, pushing the teams to bring all systems up immediately to minimize financial impact.

Outcome: Financial metrics recover quickly, but unresolved security debt leaves you open to future pivots.

`-1 Stakeholder Communication` `+2 Business Continuity`

PHASE 4 - GOVERNANCE & MATERIALITY • CHIEF INFORMATION SECURITY OFFICER +0S

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

Decision: Identify specific individuals whose decisions contributed to the delay, for the board's satisfaction.

Outcome: The board feels accountability was served, but the team becomes visibly more reluctant to report problems early next time.

`-2 Stakeholder Communication` `+1 Regulatory Posture`

PHASE 4 - GOVERNANCE & MATERIALITY • CHIEF INFORMATION SECURITY OFFICER +0S

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: Full disclosure: confirm the ransomware attack, the confirmed data exposure, and detail the specific architecture changes being made.

Outcome: The statement is thorough and gets ahead of every open question - at the cost of putting technical specifics about your defenses on the public record for competitors and future attackers to read.

`+2 Stakeholder Communication` `+2 Regulatory Posture` `-1 Business Continuity`

PERFORMANCE ASSESSMENT

Containment Effectiveness	7/10
Stakeholder Communication	4/10
Regulatory Posture	6/10
Business Continuity	6/10
Data Exposure	Not Confirmed

OBSERVATIONS

Strengths

- Containment Effectiveness performed well (7/10), reflecting effective decisions across the exercise.

Areas of Concern

- Stakeholder Communication scored 4/10, indicating an area for focused improvement.

IMPROVEMENT PLAN

IDENTIFIED GAP	RECOMMENDED TRAINING MODULE	RATIONALE	OWNER	TARGET DATE
Executive Crisis Communication	Executive Security Program Leadership	Stakeholder confidence took a hit during the response — clearer, faster communication under pressure is a leadership skill worth sharpening.		

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	Wait for SOC's preliminary scope assessment before looping in anyone outside the crisis bridge.	containmentSpeed: +1, stakeholderTrust: -1
Phase 2	Chief Information Security Officer	Say nothing publicly and just quietly work the phones with your biggest customers one-on-one.	stakeholderTrust: -1, businessContinuity: +1
Phase 2	Chief Information Security Officer	Decline to estimate until finance can produce a verified figure, even if the board pushes back.	regulatoryStanding: +1, stakeholderTrust: -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 3	Chief Information Security Officer	Refuse negotiation entirely, and direct the recovery team to focus solely on backup restoration.	stakeholderTrust: +1, businessContinuity: -1
Phase 3	Chief Information Security Officer	Contact the competitors' business leadership informally, framed as a professional courtesy heads-up.	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 4	Chief Information Security Officer	Commit to a fast resume-work date, pushing the teams to bring all systems up immediately to minimize financial impact.	stakeholderTrust: -1, businessContinuity: +2
Phase 4	Chief Information Security Officer	Identify specific individuals whose decisions contributed to the delay, for the board's satisfaction.	stakeholderTrust: -2, regulatoryStanding: +1
Phase 4	Chief Information Security Officer	Full disclosure: confirm the ransomware attack, the confirmed data exposure, and detail the specific architecture changes being made.	stakeholderTrust: +2, regulatoryStanding: +2, businessContinuity: -1