Grimlin

After-Action Report

Operation Iron Horizon · July 16, 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 Business Continuity, scoring 7 out of 10. The most significant gap identified was Regulatory Posture, 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	Solo
Date	July 16, 2026
Duration	1 minute
Participants	Dan (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.

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

TIMELINE OF DECISIONS

ACT 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.

ACT 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.

ACT 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.

ACT 4 - GOVERNANCE & MATERIALITY • CHIEF INFORMATION SECURITY OFFICER

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.

PERFORMANCE ASSESSMENT

Containment Effectiveness		6/10
Stakeholder Communication		6/10
Regulatory Posture		4/10
Business Continuity		7/10
Data Exposure	Confirmed	

OBSERVATIONS

Strengths

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

Areas of Concern

- Regulatory Posture scored 4/10, indicating an area for focused improvement.

IMPROVEMENT PLAN

IDENTIFIED GAP	RECOMMENDED TRAINING MODULE	RATIONALE	OWNER	TARGET DATE
Regulatory & Data Governance Response	Data Governance & Loss Prevention	Your handling of disclosure timing and regulatory posture during the incident could be stronger.		
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

ACT	ROLE	DECISION	STATE DELTAS
Act 1	Chief Information Security Officer	Declare a P1 corporate incident immediately, spin up the crisis bridge, and notify executive leadership.	stakeholderTrust: +1, containmentSpeed: +1
Act 2	Chief Information Security Officer	Release a transparent statement acknowledging a cybersecurity incident and confirming containment is underway.	stakeholderTrust: +2, regulatoryStanding: -1
Act 3	Chief Information Security Officer	Authorize the negotiator to offer a token payment to delay the leak site countdown.	stakeholderTrust: -1, dataExposureConfirmed: true
Act 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

Generated by Grimlin on July 16, 2026.