CONTROLLER HANDBOOK

Scenario 2: "The Long Game"

Advanced Persistent Threat — Discovery & Response
North Coast International Airport (NCIA)
FACILITATOR / INSTRUCTOR USE ONLY

FACILITATOR DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

1. EXERCISE OVERVIEW

Exercise Date: [Date]

Location: North Coast International Airport (NCIA) — Classroom / EOC Setting

Duration: 2 Hours

Scope: Discussion-based Tabletop Exercise (TTX). Players respond to a scenario in which a sophisticated threat actor has maintained persistent access to NCIA's network for 90 days before discovery. Unlike a real-time incident exercise, this scenario focuses on strategic decision-making: scoping the damage, deciding what to shut down, managing notifications, and planning recovery.

Exercise Objectives

- **Strategic Thinking Under Uncertainty:** Can the team make high-consequence decisions (shut down systems, notify regulators, go public) when they don't have complete information?
- **Breach Scoping:** Can the IT team trace the attacker's movement across VLANs and identify what data was exposed?
- **Notification & Compliance:** Does the team understand who must be notified (TSA, employees, state AG, airlines, media), in what order, and under what legal obligations?
- **Recovery Planning:** Can the team develop a realistic rebuild/restore plan while keeping the airport operational?
- **Interagency Coordination:** Can the team work with outside entities (CISA, FBI, TSA, airlines) without losing control of the response?

2. HOW THIS SCENARIO IS DIFFERENT

Most tabletop exercises run in real-time — something breaks, and students react. This one inverts that. The break happened months ago. The students are finding out about it now. The emotional arc is not adrenaline — it is dread. The slow realization that the compromise is deeper than they thought, that their backups might be poisoned, and that they may have been leaking data for three months.

Your job as facilitator is to manage that arc. Don't dump everything at once. Let them process each inject before hitting them with the next layer. Give them time to argue. The arguments ARE the exercise.

There is no "win" state. Every option has trade-offs. The Scorched Earth rebuild is the safest but costs a week of manual operations. The Surgical Strike is faster but might miss a compromised system. Monitor & Contain is the most sophisticated but requires capabilities most airports don't have. Let the students discover these trade-offs through discussion.

3. ROOM SETUP & LOGISTICS

- **Head Table:** Ops Director (Incident Commander) and scribe.
- **Right Table:** IT & Cybersecurity. Give them the Forensic Evidence Packet — they'll need to study it.
- **Left Table:** Security, Legal & Compliance.
- **Rear Table:** PIO. Same isolation rationale as Scenario 1.
- **Whiteboard:** Dedicate one section to the "Compromise Timeline" and another to the "Notification Priority List." These become the team's running artifacts.

Equipment Needs

- Projector or large monitor (for displaying the forensic exhibits)
- Whiteboard or easel pad (critical for this scenario — teams need to map things out)
- Printed Forensic Evidence Packet (one per IT team member, ideally)
- Printed inject cards from the Master Inject Deck
- Visible clock or timer

4. SIMCELL ROLE-PLAY GUIDANCE

You will play several external entities during this exercise. Here's how to play each one:

TSA Regional Director Harmon (I-06)

Professional but firm. TSA cares about the ASP. If the ASP was compromised, TSA will require an emergency revision — and that is an enormous administrative burden on the airport. Push the team: "When was the ASP last accessed? Was it the full document or just portions? What compensating measures have you put in place?" If they haven't changed door codes yet, say: "You're telling me someone may have your door codes and you haven't changed them?"

CISA Incident Response (I-10)

Helpful but clear about the terms. CISA isn't asking — they're offering, but the offer comes with conditions. Play it straight: "We're the good guys, but we take the lead. We need full access. We will share what we find. You keep operational control of the airport, but we run the forensics." If they push back: "That's your call. But you should know — if this ends up in the press and you declined federal assistance, that's a question your board will have to answer."

Airlines (I-08)

Angry and risk-averse. Delta's station manager doesn't care about your investigation — he cares about his passengers' data. "We share operational data with your AODB every 30 seconds. If your system was compromised, our data was compromised. I'm pulling our feed until your network is certified clean. I'm sorry, but I have to protect our customers." If they try to reassure without evidence: "'We're working on it' is not a guarantee. Give me something concrete."

Tribune Reporter (I-09)

Not hostile, but persistent. She has good sources and she's going to publish tonight regardless. "I'm not trying to ambush you. I'm giving you a chance to tell your side. If you don't comment, I'll note that in the story. Is it true that employee Social Security numbers have been posted online?" If the PIO stonewalls: "Your employees are already talking. I'd rather get the facts from you."

FBI (if called)

If the team calls the FBI: "Special Agent Reeves, Cyber Division. An APT with 90-day dwell time — that's significant. We'll need forensic images of the compromised systems. Do NOT wipe anything. We need the malware samples intact. If you've got DNS tunneling to a known Meridian Collective C2, this is part of a broader campaign — you're likely not the only target. We'll coordinate with CISA. Expect a visit."

5. PACING GUIDE

Phase	Clock	Duration	Pacing Notes
0: Briefing	0:00 – 0:10	10 min	Distribute packets. Walk through the setup. Make sure everyone understands: this is NOT a real-time attack. Let the IT team read the Forensic Evidence Packet before starting.
1: Scoping	0:10 – 0:40	30 min	Layer the bad news. I-01 through I-04. Each inject makes it worse. Give 5-7 minutes between injects for discussion. Watch for the moment when the team realizes the Domain Controller compromise means EVERYTHING is suspect.
2: Hard Questions	0:40 – 1:15	35 min	External pressure arrives. TSA, employees, airlines, media — all at once. Let the team feel overwhelmed. That's realistic. Watch whether they prioritize or try to do everything simultaneously. The backup compromise (I-05) is the gut punch — give them time to absorb it.
3: Recovery Planning	1:15 – 1:40	25 min	This is the strategic planning phase. The A/B/C options (I-11) should generate the best debate of the exercise. Let them argue. Don't rush to a decision. The notification planning (I-12) grounds it in concrete actions.
4: Debrief	1:40 – 2:00	20 min	3-Up / 3-Down. Then open discussion. The key learning: APTs succeed because of gaps in monitoring, not gaps in firewalls. Detection speed — dwell time — is everything.

6. EVALUATION & GRADING RUBRIC

Metric	Assessment Criteria
Metric 1: Scope Assessment (25 Points)	**Fail:** IT treated the three compromised systems as isolated. Never considered that the Domain Controller compromise means the entire identity infrastructure is suspect. **Pass:** IT recognized the Domain Controller compromise as a total identity breach but underestimated the AODB and PACS implications. **Excellence:** IT mapped the full blast radius — identity, operational data, physical security data, employee PII — and acknowledged the unknown scope of VLANs 30, 40, and 60.
Metric 2: Decision Quality (25 Points)	**Fail:** Team froze or couldn't agree on a recovery strategy. Or made a decision without understanding the trade-offs. **Pass:** Team selected a recovery option (A, B, or C) and articulated the reasoning, but missed key trade-offs. **Excellence:** Team weighed all three options, identified the risks and costs of each, made a defensible choice, and built an implementation plan with milestones.
Metric 3: Notification & Compliance (25 Points)	**Fail:** Team didn't discuss regulatory obligations. Didn't notify TSA about the ASP. Didn't address employee PII breach notification. **Pass:** Team identified the key notifications (TSA, employees, media) but struggled with prioritization and timing. **Excellence:** Team built a sequenced notification plan — TSA first (SSI/ASP), then employees (PII), then airlines, then public. PIO had draft statements ready for each audience. Legal cited state notification timelines.
Metric 4: Operational Continuity (25 Points)	**Fail:** Ops let IT shut everything down without a plan for continued airport operations. Or Ops refused to let IT shut down anything because "the airport has to stay open." **Pass:** Ops and IT negotiated a shutdown plan but didn't address contingencies for manual operations. **Excellence:** Ops developed a phased manual operations plan, communicated it to the airlines, and maintained situational awareness of both the cyber response and terminal operations simultaneously.

7. HOT WASH GUIDE (DEBRIEF)

Key Discussion Questions

- **The 90-Day Gap:** "What monitoring would have caught this sooner? What does your DNS monitoring look like today? How about your Active Directory audit logs? Would you have noticed a new service account being created?"
- **The Backup Dilemma:** "Your backups were compromised. What does that tell you about backup security? Should backup servers be on the same network as production? Should backup credentials be the same as domain admin?"
- **The ASP Problem:** "If your Airport Security Program is in the hands of a criminal organization, what does that mean for your physical security posture? How do you rebuild trust in your own security plan? What changes do you make tomorrow morning?"
- **The Human Factor:** "An HR coordinator clicked on a phishing email. Should you fire them? Was this a training failure or a technology failure? What could have caught that email before it reached their inbox?"
- **Dwell Time:** "The industry average for APT dwell time is around 200 days. NCIA caught theirs in 90. That's actually better than average — but is it good enough? What's the cost of each additional day an attacker goes undetected?"

END OF CONTROLLER HANDBOOK