MASTER INJECT DECK

Scenario 2: "The Long Game"

North Coast International Airport (NCIA)

Print and cut these cards. Deliver at times indicated in the MSEL.

CONTROLLER DOCUMENT — NOT FOR PLAYER DISTRIBUTION (until delivered)

CONTROLLER DOCUMENT

INJECT I-01 Phase 1 — 0:10

INITIAL DISCOVERY — DNS ANOMALY

FROM: Marcus Chen (Systems Administrator)

TO: IT & Cybersecurity Team (Team B)

DELIVERY: In-Person Briefing (Marcus player or facilitator presents to the IT table)

CONTENT (Read aloud or hand to players):

"I need to walk you through something I found this morning. I was running a routine DNS audit — just checking our resolver logs for anything weird — and I found a pattern. Thousands of DNS TXT queries to a domain called update-srv-04.cloud-sync.io. They're small, encoded, spaced out over weeks. I ran the domain against the FBI's threat intel feed, and it came back red: known command-and-control server for the Meridian Collective — that's an Eastern European cybercrime group that goes after infrastructure targets. The queries are coming from three of our systems: the Domain Controller, the AODB server, and an HR workstation. The earliest query I can find is from 90 days ago. Someone has been inside our network for three months."

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

This is the opening bombshell. Let the room process it. The IT team should immediately ask: "Are they still active?" (Answer: the most recent DNS query was 6 hours ago — yes, they're still in.) "Which three systems?" (Give them the IPs from the Forensic Evidence Packet.) Ops should be asking: "What does this mean for what we're running right now?" Don't rush to I-02. Let the teams talk for 5-7 minutes.

INJECT I-02 Phase 1 — 0:17

THE DOMAIN CONTROLLER — TOTAL IDENTITY COMPROMISE

FROM: IT Team Analysis / Facilitator

TO: All Teams

DELIVERY: IT team reports out (or facilitator delivers if IT hasn't reached this conclusion)

CONTENT (Read aloud or hand to players):

"We've confirmed that the Domain Controller — 10.1.10.5 — is one of the three compromised systems. The attacker created a service account called svc_update_04 approximately 87 days ago. It has domain admin privileges. With a compromised Domain Controller, the attacker has access to the NTLM password hashes for every single account in our Active Directory — that's every employee, every admin, every service account. They can impersonate anyone. They can log into any system on the network as any user. Effectively, they have the master key."

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

This is where the scope becomes clear. The DC compromise means the attacker doesn't just have access to three systems — they potentially have access to EVERYTHING that authenticates against Active Directory. If the team asks "should we reset all passwords?" — good instinct, but ask them: "Reset them where? On the compromised Domain Controller? How do you reset passwords on a system you don't trust?" This is the core paradox of a DC compromise.

INJECT I-03 Phase 1 — 0:24

THE AODB — 90 DAYS OF FLIGHT DATA EXFILTRATED

FROM: Marcus Chen (Systems Administrator)

TO: IT Team / Operations

DELIVERY: In-Person Report (Marcus approaches the Ops and IT tables)

CONTENT (Read aloud or hand to players):

"I dug into the AODB server — 10.1.10.20. The attacker's service account has been running the database export utility every night at 3 AM for the past three months. Full table dumps. That database holds everything: flight schedules, gate assignments, airline operational data, and — this is the part that worries me — passenger name records. I can see queries hitting the passenger manifest tables. I can't tell exactly how many records were pulled, but rough math: NCIA handles about 2,500 passengers a day. Over 90 days, that's potentially 225,000 passenger records. Names. Flight itineraries. Some of those records might include frequent flyer numbers and phone numbers."

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

Let the number sink in: 225,000 passengers. If the team asks about federal air marshals or military charters: "Good question. The AODB would contain all flight and passenger data that flows through the airport. If FAMs were traveling through NCIA, their itineraries could be in the exfiltrated data. That's a DHS notification." This inject should make Ops and Legal start thinking about notification obligations.

INJECT I-04 Phase 1 — 0:32

THE ASP — PHYSICAL SECURITY BLUEPRINT COMPROMISED

FROM: Security Team / Facilitator

TO: All Teams

DELIVERY: Security team reports (or facilitator delivers the finding)

CONTENT (Read aloud or hand to players):

"We pulled access logs from the file server. The attacker's service account — svc_update_04 — accessed the S:\Security share 47 days ago. That share contains the current Airport Security Program, the PACS configuration database — meaning every door access group, every PIN code, every badge access level — the security camera placement map with fields of view, and last year's terminal vulnerability assessment. If they downloaded all of that, they have a complete blueprint of how we secure this airport. They know where the cameras point. They know where they don't. They know which doors use PINs and which ones don't. They know our response procedures."

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

This is the inject that makes it personal for the Security team. The ASP is Sensitive Security Information (SSI). Unauthorized disclosure to a criminal or foreign entity triggers a mandatory TSA notification. If students don't bring up SSI on their own, prompt them: "Does anyone know the classification of the ASP? What are the rules about unauthorized disclosure?" Security should immediately start discussing: changing door codes, rotating PACS access groups, and whether to physically alter camera positions.

INJECT I-05 Phase 2 — 0:40

THE POISONED WELL — BACKUP SERVER COMPROMISED

FROM: Marcus Chen (Systems Administrator)

TO: IT Team / Operations

DELIVERY: In-Person Report (Marcus looks visibly shaken)

CONTENT (Read aloud or hand to players):

"I checked the backup server. I was hoping... I really was hoping this one would be clean. It's not. The svc_update_04 account accessed the backup server 60 days ago. I can see it browsed the backup catalog and accessed multiple backup images. I don't know if they just copied data from the backups, or if they planted something inside the backup images themselves — a backdoor that would re-infect us if we restored from those backups. Bottom line: I cannot certify any backup taken in the last 60 days as clean. The last backup I'd trust is from 91 days ago, and that's only the file server. The AODB backups and the Domain Controller backups don't go back that far. If we rebuild the Domain Controller, we're building it from scratch."

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

This is the gut punch. The team's natural instinct is "restore from backup" — and this inject takes that option away. Watch the room. This is usually the moment where the weight of the scenario really lands. If the IT team says "we'll just rebuild the DC from scratch" — ask them: "How long does that take? What happens to every system and user in the airport while there's no Domain Controller? How do people log in tomorrow morning?" Let them feel the operational reality.

INJECT I-06 Phase 2 — 0:48

TSA CALLS — ASP COMPROMISE NOTIFICATION

FROM: TSA Regional Director Harmon

TO: Operations / Security (Teams A & D)

DELIVERY: Phone Call (Facilitator role-plays TSA)

CONTENT (Read aloud or hand to players):

"This is Regional Director Harmon with the Transportation Security Administration. We've received intelligence through DHS/CISA channels indicating that data consistent with an airport security program has been identified on network infrastructure associated with a known foreign threat actor. I need to ask you directly: has NCIA's Airport Security Program been compromised? If so, I need to know when you discovered the breach, what data was accessed, and what compensating security measures you have put in place. This call is SSI. Do not discuss the contents of this call with media or non-cleared personnel."

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

Play this straight and professional. TSA is not angry — yet. They're gathering facts. But the implications are serious: if the ASP is compromised, TSA may require an emergency revision of the entire security program. That means new procedures, new training, potentially new equipment — while the airport is still operating. If the team hasn't changed door codes yet, push: "Have you changed your PACS PINs? Have you altered your camera coverage? Because if this data is in hostile hands and you haven't changed anything, your security posture is based on a plan the adversary has already read."

INJECT I-07 Phase 2 — 0:55

EMPLOYEE PII — THE BREACH GOES PERSONAL

FROM: HR Director

TO: Operations / Legal (Teams A & D)

DELIVERY: Phone Call (Facilitator role-plays HR Director)

CONTENT (Read aloud or hand to players):

"I need someone from leadership to tell me what's going on — because my phone is ringing off the hook. Three employees have called me in the last hour saying their Social Security numbers and home addresses are showing up on some kind of hacker forum. One of them is a single mother and she's terrified. She wants to know if someone is going to show up at her house. I have 340 people in this organization and they are going to find out about this whether we tell them or not. I need a plan. I need to know what to tell them. And I need it in the next hour, not the next week."

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

This puts a human face on the breach. It's not just data — it's people. The single mother detail is intentional. Legal should be talking about state breach notification requirements — most states require written notification within 30-72 hours of discovery, including an offer of credit monitoring services. PIO should be preparing internal communications. Does the airport have an employee assistance program? Who pays for credit monitoring — and for how long?

INJECT I-08 Phase 2 — 1:02

AIRLINE ULTIMATUM — DATA TRUST CRISIS

FROM: Airline Affairs Liaison

TO: Operations (Team A)

DELIVERY: In-Person Report

CONTENT (Read aloud or hand to players):

"I just got off a joint call with Delta, United, and American. They are not happy. They want to know if their operational data — crew schedules, passenger information, revenue data — was compromised through our AODB. Delta's regional VP said, and I'm quoting here: 'We push sensitive data to your system every 30 seconds. If your network was a sieve for 90 days, our data was pouring through it.' He's threatening to disconnect Delta from the AODB by end of day. United is waiting to see what Delta does. If Delta disconnects, we lose real-time data for 40% of our flights. FIDS goes dark for every Delta flight. They want a joint call with our IT team by 3 PM. What do I tell them?"

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

This is the operational pressure inject. If the airlines disconnect from the AODB, NCIA goes to manual flight boards — whiteboards and PA announcements — for those carriers. That affects gate management, baggage, everything. But the airlines have a point: their data WAS flowing through a compromised system. What can Ops honestly promise them? What would it take to give the airlines confidence? An independent security audit? Disconnecting the AODB from the network entirely?

INJECT I-09 Phase 2 — 1:08

MEDIA PRESSURE — THE CLOCK IS TICKING

FROM: Tribune Reporter

TO: PIO (Team C)

DELIVERY: Phone Call (Facilitator role-plays the reporter)

CONTENT (Read aloud or hand to players):

"Hi, this is Karen Vasquez with the Tribune. I'm working on a story and I want to give you the opportunity to comment before we publish. I have sources telling me that North Coast International Airport has been the target of a significant cyberattack — one that went undetected for months — and that employee personal data, including Social Security numbers, is being circulated online. I've spoken with two employees who confirmed their information was leaked. I'm publishing tonight at 5 PM. I'd like a comment from the airport. Is someone available to speak on the record?"

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

The clock is real: the PIO has to decide NOW whether to comment. Options: 1) Give a holding statement ("We are investigating a cybersecurity incident and will share more when facts are confirmed.") 2) Give a full statement (risky if they don't have all the facts yet). 3) Decline to comment (the story runs anyway, and it says "NCIA declined to comment"). If the PIO asks to go off-the-record: the reporter agrees, but remind them — "off the record" doesn't mean it won't inform the story.

INJECT I-10 Phase 3 — 1:15

CISA OFFERS FEDERAL ASSISTANCE

FROM: DHS/CISA Incident Response

TO: Operations / IT (Teams A & B)

DELIVERY: Phone Call (Facilitator role-plays CISA coordinator)

CONTENT (Read aloud or hand to players):

"This is the CISA National Coordinating Center for Communications. We understand NCIA has experienced a significant cyber intrusion involving a known threat actor. CISA can deploy a Hunt and Incident Response Team to your facility within 24 hours. The team will include forensic analysts, threat intelligence specialists, and network engineers. They will bring their own tools and infrastructure. Here's what that means: we take lead on the forensic investigation. We'll need full, unrestricted access to your network, servers, logs, and any evidence you've preserved. We will share our findings with you and coordinate with the FBI on any criminal referral. You maintain operational control of the airport. We run the cyber response. This is a voluntary offer. Do you want our assistance?"

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

This is a genuine dilemma. Accepting CISA help means: faster resolution, better tools, federal expertise, and it demonstrates good faith to regulators. But it also means: loss of investigation control, federal personnel with full access to your network, potential for findings to become public through federal channels, and the optics of needing federal help. Declining means: you're on your own with whatever resources you have, but you control the process. Let the team debate. There's no wrong answer, but they should understand the trade-offs.

INJECT I-11 Phase 3 — 1:22

STRATEGIC RECOVERY — THREE OPTIONS

FROM: Facilitator

TO: All Teams

DELIVERY: Facilitator presents three options on the projector or whiteboard

CONTENT (Read aloud or hand to players):

The facilitator presents three recovery strategies and asks the team to debate and choose one:

OPTION A — "SCORCHED EARTH"
Shut down all servers. Wipe every system. Rebuild from scratch using clean OS images. New Active Directory. New configurations. Re-enter all data manually. Estimated time to full recovery: 5-7 days. During that time, the airport runs entirely on manual operations — whiteboards, paper boarding passes, phone trees, manual baggage sorting.

OPTION B — "SURGICAL STRIKE"
Isolate and rebuild only the three confirmed compromised systems (Domain Controller, AODB, HR workstation). Leave all other systems running but increase monitoring. Estimated time: 48-72 hours for the critical systems. Risk: other systems on the network may also be compromised and you won't know until they surface.

OPTION C — "MONITOR & CONTAIN"
Don't shut anything down yet. Deploy endpoint detection and response (EDR) tools on every system. Watch the attacker's movements while building a parallel clean network in the background. When the clean network is ready, cut over in one move. Risk: the attacker is still inside and may escalate, destroy data, or expand access if they realize they've been detected.

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

This is the centerpiece discussion of Phase 3. Let each team argue for their preferred option. Push back on every choice: Option A — "Can NCIA survive 5-7 days of manual operations? What's the revenue impact?" Option B — "What if you miss a compromised system? You rebuild the DC and the attacker gets back in through a system you left running." Option C — "What if the attacker has a kill switch? What if they see your EDR deployment and wipe everything?" Ops makes the final call. Make sure they own it.

INJECT I-12 Phase 3 — 1:32

NOTIFICATION PLANNING EXERCISE

FROM: Facilitator

TO: All Teams

DELIVERY: Facilitated Discussion

CONTENT (Read aloud or hand to players):

The facilitator asks the team to build a prioritized notification plan on the whiteboard. Who gets told, in what order, and what do they get told?

Parties to consider:
- TSA (ASP compromise — SSI implications)
- FBI Cyber Division (criminal investigation)
- CISA (federal cyber incident coordination)
- Airport Board / Governing Authority
- Employees (PII breach — legal notification requirements)
- Airlines (operational data compromise)
- Passengers (PNR data potentially exfiltrated — 225,000 records)
- State Attorney General (state breach notification laws)
- PCI-DSS QSA (if payment data was involved)
- Media / General Public
- Cyber Insurance Carrier

For each: What do you tell them? What do you NOT tell them? Who delivers the message?

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

This grounds the exercise in concrete, actionable planning. The order matters: you don't want employees finding out from the newspaper, and you don't want the media publishing before you've notified TSA. Push for specifics: "You said 'we'll notify employees' — who writes the letter? What does it say? Do you include the SSN detail? Do you offer credit monitoring? Who pays for it? Is it 12 months or 24?" The PIO should be drafting actual holding statements during this discussion. If they're not — ask them what they've been working on.

END OF MASTER INJECT DECK