SCENARIO 2: "THE LONG GAME"

Cybersecurity Incident Response & Recovery

North Coast International Airport (NCIA)
Tabletop Exercise — Player Briefing Packet
Exercise Duration: 2 Hours
EXERCISE — FOR TRAINING USE ONLY

EXERCISE — EXERCISE — EXERCISE

1. SITUATION BRIEF

This exercise is different from a typical tabletop. We are not starting at the beginning of a crisis. We are starting in the middle of one — after the worst part has already happened without anyone knowing.

It is 8:00 AM on a Monday morning. The airport is operating normally. Flights are on time. Passengers are moving through the terminal. Nothing looks wrong.

Twenty minutes ago, NCIA's Systems Administrator — Marcus Chen — was reviewing DNS query logs as part of a routine security audit. He noticed a pattern: thousands of DNS queries over the past several weeks to a domain called **update-srv-04.cloud-sync.io**. The queries were small, encoded, and spaced out to avoid triggering volume alerts. Marcus checked the domain against a federal threat intelligence feed. It came back flagged as a known **command-and-control (C2) server** associated with an organized cybercrime group.

Marcus pulled the thread. The DNS queries are coming from **three different systems** inside NCIA's network. The earliest query he can find in the retained logs dates back **approximately 90 days**.

Someone has been inside your network for three months. You just found out this morning.

YOUR MISSION: Determine the scope of the compromise, decide what to shut down and what to keep running, figure out who needs to be notified, and build a recovery plan — all while keeping the airport operational.

System	Status
Terminal / Airfield	Normal Operations — but trust level is now unknown
FIDS / PA / BHS	Functioning — integrity unverified
PACS / Access Control	Functioning — integrity unverified
IT Network	Compromised — scope unknown
Backup Systems	Status unknown — may be compromised
Email / Admin Systems	Functioning — assume attacker can read email

2. KEY CONCEPT: WHAT IS AN APT?

An **Advanced Persistent Threat (APT)** is not a smash-and-grab. It is not ransomware that locks your screens and demands Bitcoin. An APT is a long-term, stealthy intrusion by a sophisticated actor — often a criminal organization or nation-state — whose goal is to maintain access to your network for as long as possible, quietly collecting data.

APT actors are patient. They move slowly. They use legitimate admin tools to blend in with normal traffic. They don't trip alarms because they look like your own people. The average time between an APT gaining access and being discovered — the "dwell time" — is measured in months, not minutes.

The challenge you face today is not "stop the attack." The attack happened 90 days ago. Your challenge is: **What do you do now?**

3. TEAM ASSIGNMENTS & STANDING ORDERS

TEAM A: AIRPORT OPERATIONS (COMMAND)	
Role: You are the Incident Commander. Every system in this airport might be compromised — but you still have flights to run, passengers to move, and a business to operate. Your job is to balance security with continuity. IT will want to shut things down. Airlines will want guarantees. You have to make the hard calls.	**Standing Orders:** Continuity: The airport stays open unless there is a direct safety threat. Decision Authority: You authorize any system shutdowns. Coordination: Keep every team on the same page. Information silos will kill you.

TEAM B: IT & CYBERSECURITY (TECHNICAL)	
Role: You own the investigation. Marcus Chen found the thread — now you have to pull it. Which systems were accessed? What data was taken? Is the attacker still inside right now? Can you trust your backups? You will need to make recommendations to Ops, but remember: they decide, not you.	**Standing Orders:** Scope: Map every system the attacker touched. Containment: Figure out how to cut off the attacker without crashing operations. Evidence: Preserve everything. Forensic images before you change anything.

TEAM C: PUBLIC INFORMATION (PIO)	
Role: If this gets out — and it will — the story is that NCIA was hacked for three months and nobody noticed. That is a devastating headline. Your job is to get ahead of it. Draft holding statements. Prepare for the press conference nobody wants to give. Think about affected parties: passengers, employees, airlines, vendors. They all deserve to hear it from you before they hear it on the news.	**Standing Orders:** Prepare: Draft statements for multiple audiences before you need them. Notify: Work with Legal on breach notification timelines. Control: One voice. One message. No freelancing.

TEAM D: SECURITY, LEGAL & COMPLIANCE	
Role: This is a crime. It may also be a regulatory event. If the PACS system was accessed, your physical security posture is compromised — someone out there may know every door code and camera blind spot at this airport. If employee PII was taken, you have breach notification obligations. If the ASP was accessed, TSA needs to know immediately. You also need to think about law enforcement coordination — FBI, CISA, possibly Secret Service.	**Standing Orders:** Physical Security: Assess whether PACS/camera data was exfiltrated. Regulatory: Identify every notification obligation (TSA, state AG, PCI, etc.). Law Enforcement: Coordinate with FBI/CISA without losing control of the investigation.

4. RULES OF ENGAGEMENT

- **"This is an Exercise":** Begin and end all simulated communications with this phrase.
- **Real-World Emergencies:** Use **"REAL WORLD — REAL WORLD"** to halt the exercise for any actual emergency.
- **Time Compression:** This exercise covers decisions that would unfold over days or weeks. The facilitator will compress time. When they say "It is now 48 hours later," adjust your thinking.
- **Injects:** You will receive forensic reports, emails, phone calls, and news articles. Treat them as real.
- **No Perfect Answers:** This scenario has no clean solution. Every option involves trade-offs. The goal is not to "win" — it is to make defensible decisions under uncertainty and communicate them clearly.
- **Assume the Attacker Can Hear You:** The attacker may still have access to email, internal chat, and network monitoring tools. Think about operational security — how do you coordinate a response when your own communications infrastructure might be compromised?

5. INCIDENT BRIEFING FORM (ICS-201)

Use this form to track the situation as it evolves.

COMPROMISE TIMELINE
(What do we know about the attacker's activity over the last 90 days? Build a timeline.)

CRITICAL DECISIONS TRACKER
Decision 1: _____ (Shut down / Keep running? Which systems?)
Decision 2: _____ (Who do we notify first? In what order?)
Decision 3: _____ (Restore from backup or rebuild from scratch?)
Decision 4: _____ (When do we go public?)

System	Accessed by Attacker?	Data at Risk	Decision: Keep / Kill / Rebuild
Domain Controller			
AODB / FIDS Server			
PACS / Access Control			
Payment Gateway			
Email Server			
File Server			
Backup Server			
NVR / CCTV			
Baggage Handling System			

EXERCISE — EXERCISE — EXERCISE

End of Player Briefing Packet