SCENARIO 1: "GLASS HOUSE"

Network Security & Incident Response

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

It is a busy Wednesday afternoon at North Coast International Airport. Operations are normal. The terminal is moderately crowded with a mix of business travelers and families heading out for the week. All airport systems — FIDS, baggage handling, access control — are functioning normally.

Terminal Status	Normal Operations
Airfield Status	Green / Open
IT Systems	Green / Normal
Staffing	Full shifts — Ops, Maintenance, IT, Security
Weather	Overcast, 52°F. Light rain. Winds SW at 8 kts.

The Initial Report

At 1:00 PM, the Airport Operations Center (AOC) receives three calls in quick succession. The SkyLounge (the premium airline lounge in Concourse B) and two duty-free shops in Concourse A are reporting that credit card transactions are taking 25–30 seconds to process instead of the usual 2–3 seconds. Customers are getting impatient. One shop manager says a few customers have walked away from purchases. Another says some transactions are being declined outright, even though the customer insists the card is good.

Your IT Manager, **Jordan Kelley**, is already aware of the complaints. Kelley is on-site today and has told the AOC it is "probably an ISP latency issue" and that a call to the internet provider is underway.

YOUR MISSION: Investigate the source of the transaction delays, determine whether passenger financial data is at risk, maintain airport operations, and coordinate with all stakeholders as the situation develops.

2. TEAM ASSIGNMENTS & STANDING ORDERS

TEAM A: AIRPORT OPERATIONS (COMMAND)	
Role: You own the physical airport. Passenger safety and business continuity are your priorities. You are the "client" — you tell IT what you need, and you decide when to escalate. If vendor operations are degraded, figure out workarounds. Keep the concession tenants informed. If something smells wrong, trust your gut — you have the authority to escalate.	**Standing Orders:** Safety First: Protect passengers and employees. Continuity: Keep the airport running. Vendors need to do business. Escalation: If the scope grows beyond a "tech glitch," activate the appropriate response plan.

TEAM B: IT & CYBERSECURITY (TECHNICAL)	
Role: You own the network. Your job is to find out why transactions are crawling — and whether this is a technical hiccup or something worse. Map the data flow. Check the logs. Look at network traffic. Don't accept easy answers. Your IT Manager, Jordan Kelley, will be feeding you information and suggestions. Evaluate everything critically.	**Standing Orders:** Verify: Do not accept "it's a glitch" without evidence. Contain: If you find a breach, stop the bleeding before you clean up. Preserve: Logs are evidence. Don't overwrite them. Don't reboot unless it's life-safety.

TEAM C: PUBLIC INFORMATION (PIO)	
Role: You own the narrative. If credit card data is compromised, this becomes front-page news. Customers will be angry. Airlines will want answers. The press will smell blood. Your job is to control the message, monitor social media, and make sure nobody says "data breach" on camera until you know it's true.	**Standing Orders:** Monitor: Watch social media for passenger complaints. Hold the Line: Use holding statements until facts are confirmed. Prepare: Draft a public statement for a worst-case scenario — have it ready before you need it.

TEAM D: SECURITY & LAW ENFORCEMENT	
Role: You own physical security and the law enforcement response. If this turns out to be a crime — theft of financial data, unauthorized network access, insider activity — you need to think about evidence preservation, witness interviews, and who had physical access to what. Keep one eye on the terminal crowd and one eye on the server rooms.	**Standing Orders:** Access Control: Who has been in and out of IT spaces today? Evidence: If Crime Scene tape needs to go up, you call it. Coordination: If the FBI or Secret Service needs to be looped in on a payment card breach, that starts with you.

3. RULES OF ENGAGEMENT

- **"This is an Exercise":** Begin and end all simulated communications with this phrase.
- **Real-World Emergencies:** If a real emergency occurs (medical issue, fire alarm, etc.), use the phrase **"REAL WORLD — REAL WORLD"** to halt the exercise immediately.
- **Simulated Time:** The facilitator may announce a time jump (e.g., "Time Jump: It is now 2:15 PM"). Adjust your situational awareness accordingly.
- **Injects:** You will receive written materials — emails, tweets, log excerpts, maintenance reports. Treat them as real intelligence. React to them as you would on the job.
- **The IT Manager:** Jordan Kelley (played by a designated student or the facilitator) is an active participant. They will offer advice, suggest actions, and respond to your questions. Treat them as you would a real colleague.
- **Phone Calls:** If you say "I'm calling the FBI" or "I'm calling the credit card processor," the facilitator will role-play that person. Have your questions ready.

4. REFERENCE: PAYMENT DATA FLOW AT NCIA

The diagram below shows how a credit card transaction moves through NCIA's network. When a customer swipes or taps a card at a Point-of-Sale (POS) terminal in any airport shop, lounge, or restaurant, the transaction data travels across the airport's internal network before reaching the external payment processor. Use this to understand where a problem — or an attacker — could sit in the chain.

STEP	COMPONENT	NETWORK LOCATION	DESCRIPTION
1	POS Terminal (Card Reader)	Retail / Vendor VLAN (VLAN 40)	Customer taps or swipes card. Terminal encrypts card data (in theory) and sends to the processing gateway.
2	Internal Processing Gateway	Server VLAN (VLAN 10)	The airport's internal server that routes payment data to the external processor. All vendor transactions funnel through here.
3	Core Switch / Firewall	Network Core	Routes traffic between VLANs and to the internet. Firewall rules control what goes in and out.
4	External Payment Processor	Internet (Off-Site)	Third-party service (e.g., Worldpay, FirstData) that authorizes or declines the card with the issuing bank.

Key Point: The gap between Step 1 (POS Terminal) and Step 2 (Internal Gateway) crosses the airport's internal network. If an attacker can position themselves between those two points — physically or logically — they can intercept transaction data in transit. This is called a Man-in-the-Middle (MitM) attack.

5. INCIDENT BRIEFING FORM (ICS-201)

Use this form to track the situation as it develops. This is your team's board of record.

MAP SKETCH
(Sketch the terminal layout. Mark affected vendor locations, server rooms, and any areas of interest.)

CURRENT SITUATION SUMMARY
(What do we know? What is broken? What is suspicious?)

CURRENT OBJECTIVES
1. _____
2. _____
3. _____

Resource	Status (G/Y/R)	Notes
POS Systems / Vendor Transactions		
Internal Network		
Payment Processing Gateway		
Passenger Wi-Fi		
FIDS / PA System		
Physical Access Control (PACS)		
Server Room Access Logs		

EXERCISE — EXERCISE — EXERCISE

End of Player Briefing Packet