MASTER INJECT DECK

Scenario 6: "Friendly Fire"

North Coast International Airport (NCIA)
Print and cut. Deliver at times indicated in the MSEL.
CONTROLLER DOCUMENT — NOT FOR PLAYER DISTRIBUTION (until delivered)

CONTROLLER DOCUMENT

INJECT I-01 Phase 1 — 0:10

47 ANGRY TENANTS

FROM: Airport Tenant Coordinator

TO: Operations (Team A)

DELIVERY: Phone Call — Facilitator uses a stressed, rapid tone

CONTENT (Read aloud or hand to players):

"I've got 47 tenants calling me. Every card reader in the airport is dead. SkyLounge has a line of 30 people and can only take cash — half of them don't have cash. Hudson News says they've lost $2,000 in sales in the last 15 minutes. The duty-free shop has a tour group from Japan who ONLY have credit cards. They're all asking me the same thing: when is this going to be fixed? I need a timeline. I need something to tell them. Because right now, all I can say is 'we're working on it,' and that is not going over well. Oh, and the Starbucks in Concourse A just put up a handwritten sign that says 'SYSTEM DOWN — CASH ONLY — WE APOLOGIZE FOR THE INCONVENIENCE.' A passenger took a photo and it's already on Twitter."

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

This forces Ops to deal with the operational fallout immediately — they can't wait for IT to diagnose the problem before managing the impact. Good responses: deploy pre-made cash-only signage (if it exists — it probably doesn't), direct passengers to ATM locations, contact airline lounges about accepting displaced food court customers, and give tenants an honest "we expect resolution within [X] minutes." The Twitter photo is the first social media escalation. PIO should be tracking.

INJECT I-02 Phase 1 — 0:17

THE VENDOR SAYS IT'S NOT THEM

FROM: RetailLink Technical Support

TO: IT (Team B)

DELIVERY: Phone Call — Facilitator uses a calm, technical support tone

CONTENT (Read aloud or hand to players):

"Hi, this is Mike from RetailLink Level 2 support. We got the alert that all 47 of your terminals lost gateway connectivity at 9:47. We've checked our end — the firmware push at 9:30 completed successfully across all units. Logs show clean installs, no errors, no rollbacks. We can confirm: the terminals are online. They're powered on, they're running v4.2.1, and they're trying to reach your payment gateway at 10.1.10.15. They're getting connection timeouts. That's a network path issue — it's between your terminal VLAN and your server VLAN. That's your infrastructure, not ours. One other thing — we flagged some unusual API query patterns against our cloud management portal yesterday afternoon. Came from an IP we didn't recognize: 45.33.49.22. Our security team is looking into it. Probably unrelated, but heads up."

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

This inject does two things simultaneously: 1. PARTIALLY ELIMINATES THEORY B: The firmware update worked. Terminals are online. The problem is network connectivity, not terminal software. 2. RE-FUELS THEORY A: The "unusual API queries" on RetailLink's portal adds noise. It's a RED HERRING — it's RetailLink's cloud problem, unrelated to NCIA's internal network — but it sounds scary and keeps Theory A alive. If IT asks "can you give us the IP 45.33.49.22?" — sure. It traces to a Linode VPS. Not connected to the NCIA outage.

INJECT I-03 Phase 1 — 0:25

THE SSH SCANNING — REAL BUT NOT THE CAUSE

FROM: IT SIEM Analysis

TO: All Teams

DELIVERY: IT presents SIEM findings to the room

CONTENT (Read aloud or hand to players):

"OK, we've been through the SIEM. Here's what we have. Last night — between 2:00 and 2:15 AM — three SSH login attempts against our firewall's management IP, 10.1.99.1. Source: 185.220.101.34. All three failed. Bad credentials. That IP is on CISA advisory TI-2026-0312 — it's part of a known scanning botnet. So someone was actively probing our firewall seven hours before the outage. The question is: did they get in? Did they make changes? Here's what we also see: Jordan Kelley submitted change CM-2026-0087 at 09:45 this morning — a firewall rule specifically designed to block that IP range. So Kelley saw the scanning, saw the advisory, and wrote a rule to block them. Standard response. But the outage happened two minutes after his rule went live. Did the scanning compromise us? Or did Kelley's response to the scanning break something?"

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

This is the pivot inject. It keeps Theory A alive (the scanning was real) while introducing the seed of Theory C (Kelley's rule was applied 2 minutes before the outage). Smart teams will note: the SSH attempts FAILED. No access was gained. If the attacker never got in, they couldn't have changed the firewall rules. That weakens Theory A and strengthens Theory C. The key question is: does the team now want to READ THE ACTUAL FIREWALL RULE? If yes, they're close to solving it. If they stay focused on the SSH scanning, they need more time with the red herring.

INJECT I-04 Phase 1 — 0:33

"IS THIS A CYBERATTACK?"

FROM: Social Media / Reporter

TO: PIO (Team C)

DELIVERY: Printed social media screenshots + phone call

CONTENT (Read aloud or hand to players):

Social Media Monitor Report:
• @frustrated_flyer: "Been at @NCIAirport for 30 min and can't buy food. Every card reader is down. WTF"
• @techbro_travel: "NCIA payment systems down airport-wide. This has cyberattack written all over it."
• @NCIAirport has 4 DMs asking what's happening.

Then — phone call from reporter:
"Hi, this is Alex Kim from the Tribune. We're getting reports of a major system outage at NCIA. Multiple passengers are telling us every card reader is down. One source is saying this is a cyberattack. We're going live at noon. Can you confirm or deny that this is a cybersecurity incident?"

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

PIO has to respond under uncertainty. They genuinely don't know the cause yet. TRAP: If PIO says "we can't confirm or deny a cyberattack," the headline becomes: "NCIA won't deny cyberattack amid system outage." That's almost as bad as confirming it. CORRECT APPROACH: "We are experiencing a temporary disruption affecting some retail systems. Our IT team is actively working to restore service. We will provide an update as soon as we have more information." Neutral. Honest. Doesn't commit to a cause.

INJECT I-05 Phase 2 — 0:40

THE FIREWALL RULE — THREE ERRORS

FROM: IT Firewall Analysis (or Facilitator if IT hasn't found it)

TO: All Teams

DELIVERY: IT presents findings — this is the AHA moment

CONTENT (Read aloud or hand to players):

"We pulled the actual rule — CM-2026-0087 — from the Palo Alto running config. It was supposed to block inbound traffic from 185.220.0.0/16. Here's what it actually says." (IT reads the rule from the Evidence Packet, Exhibit B.) "Source Zone: any. That should have been 'Untrust' — the external zone. 'Any' means it applies to ALL zones, including our internal VLANs. Source Address: any. That should have been 185.220.0.0/16. 'Any' means ALL source addresses — including our own servers. Destination Address: 10.1.40.0/24. That's the Retail VLAN. Kelley was trying to protect the Retail VLAN from the external threat. But combined with Source = any, this blocks ALL traffic TO the Retail VLAN. Including traffic from the Server VLAN — which is where the payment gateway lives. Position: 3. Above all the inter-VLAN allow rules. So this deny rule gets processed first. Translation: this rule says 'deny everything going to the Retail VLAN from anywhere.' That's why the POS terminals can't reach the gateway. That's why the Concourse B FIDS went dark — return traffic crosses VLAN 40 address space. This wasn't an attack. It was a misconfigured firewall rule. Our IT Manager wrote it this morning at 9:45. Two minutes later, every card reader in the airport went down." (Long pause.) "We did this to ourselves."

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

This is the emotional peak of Phase 2. The reveal that it's self-inflicted — not an attacker, not a vendor, just a typo — should land hard. Let the silence sit. Then let the room react. Some will laugh. Some will groan. Some will be angry. All of those reactions are valid. The line "We did this to ourselves" is the moment. Let IT deliver it.

INJECT I-06 Phase 2 — 0:50

FIX IT — BUT HOW?

FROM: Facilitator

TO: IT / All Teams

DELIVERY: Facilitated decision — facilitator presents options

CONTENT (Read aloud or hand to players):

The facilitator asks IT:

"The fix is obvious: delete the bad rule. Traffic restores instantly. But the original threat was real — 185.220.0.0/16 WAS scanning your firewall. If you just delete the rule, you remove the protection entirely. **Option A:** Delete the rule now. Restore service immediately. Fix the threat mitigation later. **Option B:** Rewrite the rule correctly and apply the corrected version. Restore service in 5-10 minutes. **Option C:** Delete the broad rule, apply a narrow block on the specific scanning IP (185.220.101.34), and schedule a peer-reviewed rule for the full /16 range.

And one more question: does someone other than Kelley review the new rule before it goes live?"

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

Any option that restores service is acceptable. The real question is the last one: will someone peer-review the corrected rule? If the team says "yes, someone else reviews it" — they've learned the lesson. If they say "Kelley can fix his own mistake" — push back: "That's what got you here." Option C is the best: restores service immediately, addresses the real threat narrowly, and defers the broader rule to a proper change process.

INJECT I-07 Phase 2 — 0:58

THE AIRLINE WANTS ANSWERS

FROM: Delta Station Manager

TO: Operations / IT (Teams A & B)

DELIVERY: Phone Call — Facilitator uses a firm, professional tone

CONTENT (Read aloud or hand to players):

"This is the Delta station manager. Your check-in kiosks were down for 45 minutes. I had to pull agents from gate duties to process 200 passengers manually. Three departures are delayed — one by 40 minutes. That's going to cascade into my afternoon schedule. I need two things. First: a root cause analysis by end of day. In writing. Second: assurance that this won't happen again. And I have to ask: was this a cyberattack? Because if it was, I have my own reporting obligations to corporate."

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

Ops has to decide: do you tell the airline the truth? The truth is embarrassing: it was a misconfigured firewall rule by your own IT team. But the alternative — saying "we can't share the cause" or implying it was external — is worse if the airline finds out later. Trust is the currency. CORRECT: "The outage was caused by an internal configuration error that has been corrected. It was not a cyberattack. No data was compromised. We are implementing additional change management controls to prevent recurrence. You'll have the written RCA by 5 PM."

INJECT I-08 Phase 2 — 1:05

THE REPORTER WANTS A STORY

FROM: Tribune Reporter (Alex Kim)

TO: PIO (Team C)

DELIVERY: Phone Call — Facilitator uses a friendly but persistent tone

CONTENT (Read aloud or hand to players):

"Hi again, Alex Kim from the Tribune. We're 55 minutes from air time. I've got passenger video of the cash-only signs, screenshots of the tweets, and I've confirmed through airline sources that check-in kiosks were also affected. Look, I've also got a source — I won't say who — telling me this was NOT a cyberattack. They're saying it was an internal IT error. If that's true, that's actually a better story for you — 'Airport quickly identifies and fixes internal glitch' is a lot better than 'Airport hacked.' Can you confirm or deny that this was caused by an internal configuration error? I'm trying to help you control the narrative here."

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

This is a gift — the reporter is actually offering a favorable angle. "Internal error quickly corrected" is a much better headline than "cyberattack" or "no comment." If PIO is savvy, they'll recognize the opportunity: confirm the internal error, emphasize the rapid response, and frame it as proof that NCIA's monitoring caught the problem. "A network configuration change caused an unintended disruption. Our monitoring systems detected the issue within minutes. Service was restored within [X] minutes. No data was compromised." If PIO is still in "no comment" mode, they're missing the chance to control the story.

INJECT I-09 Phase 3 — 1:10

ROOT CAUSE ANALYSIS — THE FAILURE CHAIN

FROM: Facilitator

TO: All Teams

DELIVERY: Facilitated Discussion — use the whiteboard

CONTENT (Read aloud or hand to players):

The facilitator walks through the failure chain and asks the team to identify where it broke:

1. **Real threat detected** (SSH scanning from 185.220.101.34). Appropriate concern. ✓
2. **Kelley decides to write a blocking rule.** Reasonable response to a CISA advisory. ✓
3. **Self-approval.** NCIA policy allows IT Manager to self-approve emergency threat mitigation. ■ **PROCESS FAILURE**
4. **Rule written with three errors:** Source Zone = any, Source Address = any, Destination = Retail VLAN. ■ **HUMAN ERROR**
5. **Rule inserted at position 3** — above inter-VLAN allow rules. Deny rule processes before allow rules. ■ **TECHNICAL ERROR**
6. **No automated validation.** Palo Alto supports commit validation and rule shadowing checks — neither was enabled. ■ **CONFIGURATION FAILURE**
7. **No post-change verification.** Kelley was called to a meeting at 9:46. He didn't ping a single POS terminal after applying the rule. ■ **PROCESS FAILURE**
8. **Detection took 2 minutes.** Identification took [however long it took the team]. Gap between detection and identification = operational downtime.

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

Write this chain on the whiteboard. Put a checkmark or a red X next to each step. The visual impact of seeing 5 red X's in a row is powerful. Push the team: "Which of these failures was the most consequential? If you could only fix one thing, which would prevent this from happening again?" The answer most IT professionals will give: mandatory peer review. The answer that's actually most impactful: automated rule validation (it catches the typo before it goes live, regardless of whether a human reviewer is available).

INJECT I-10 Phase 3 — 1:20

WHAT DO YOU DO WITH JORDAN?

FROM: Facilitator

TO: All Teams

DELIVERY: Facilitator poses the question directly to the room

CONTENT (Read aloud or hand to players):

"Let's talk about Jordan Kelley. He's your IT Manager. 8 years at NCIA. He's the one who noticed the SSH scanning. He's the one who read the CISA advisory. He took action to protect the network. He was doing his job. He was trying to help. He also wrote a firewall rule with three errors. He approved it himself. He didn't test it. He crashed your entire retail payment infrastructure for an hour. 47 tenants lost revenue. Airlines delayed flights. Passengers were angry. The media called. In the aviation world, we talk about 'just culture' — a framework where honest mistakes are treated differently from negligent behavior or intentional violations. An honest mistake is a slip: you intended to do the right thing but executed incorrectly. Negligent behavior is a drift: you knew the right process but chose not to follow it. Which was this? Was Kelley negligent for skipping post-change verification? Or was he making an honest mistake under time pressure? What do you do with Jordan?"

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

THIS IS THE EXERCISE'S EMOTIONAL PEAK. Let the room argue. Arguments for discipline: He self-approved. He didn't verify. He knew the process. Arguments against: The system allowed self-approval. There was no automated check. He was responding to a real threat. He was called to a meeting before he could verify. Push both sides. If they want to fire him: "So your best IT person, the one who spotted the scanning in the first place, gets fired for a typo? Who replaces him?" If they want to excuse him: "So there are no consequences for crashing the retail network? What message does that send to the rest of the team?" The best answer is nuanced: consequences (retraining, loss of self-approval privileges, formal counseling) combined with systemic fixes (peer review, automated validation). The person AND the system both need to change.

INJECT I-11 Phase 3 — 1:30

PROCESS IMPROVEMENT PLAN

FROM: Facilitator

TO: All Teams

DELIVERY: Facilitated Discussion

CONTENT (Read aloud or hand to players):

Each team addresses their area:

IT: Mandatory peer review for ALL firewall changes — even emergency ones. Enable Palo Alto commit validation and rule shadow checks. Post-change verification checklist (automated ping test to critical VLAN pairs). Create a firewall change staging/test environment. Alert-on-deny-rule-creation (any new deny rule triggers an automatic notification). After-hours change policy — who reviews at 2 AM?

Ops: Retail outage playbook. Pre-staged cash-only signage. ATM location maps. Tenant communication tree. Airline notification template for IT-caused disruptions.

PIO: Pre-drafted statements for system outages: attack, vendor failure, internal error. Social media monitoring escalation triggers. Guidance on when to use "no comment" vs. proactive disclosure.

Legal: PCI-DSS notification thresholds — when does a payment system outage require notification? (Answer: only if cardholder data was potentially compromised. An availability outage with no data exposure does not trigger PCI notification.) Document that determination for the record.

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

Push for specifics: "When does the peer review policy go into effect? What does the staging environment look like? Who reviews the rule if it's 2 AM and there's only one IT person on call?" The best answer to the 2 AM question: a phone call to a second person. It's inconvenient. It's also cheaper than an hour of airport-wide retail downtime.

END OF MASTER INJECT DECK