CONTROLLER HANDBOOK

Scenario 6: "Friendly Fire"

Self-Inflicted Network Outage — Misidentification Puzzle
North Coast International Airport (NCIA)
FACILITATOR / INSTRUCTOR USE ONLY

FACILITATOR DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

1. EXERCISE OVERVIEW

Duration: 2 Hours

Scope: Puzzle-driven TTX with a twist: the "attacker" is the IT team's own firewall change. The exercise teaches incident misidentification, confirmation bias, change management, and the organizational dynamics of admitting a self-inflicted error. Three plausible theories compete for the team's attention. Only one is correct.

Exercise Objectives

- **Diagnostic Rigor:** Can the IT team follow evidence instead of assumptions? Do they read the actual firewall rule, or do they chase the more exciting cyberattack theory?
- **Confirmation Bias:** The exercise is designed to exploit the team's natural tendency to see what they expect to see. External scanning + vendor issues = "it must be an attack." Do they resist that pull?
- **Change Management:** The root cause is a process failure — self-approval, no peer review, no post-change verification. Does the team identify the systemic issues or just blame the individual?
- **Crisis Communication Under Uncertainty:** Can PIO manage media and passengers without prematurely declaring a cyberattack that turns out to be a typo?
- **Accountability vs. Blame:** The Jordan Kelley question. Fire him or fix the system that let him make the mistake?

2. THE PUZZLE — SOLUTION MAP

#	Clue	What It Means	Theory Impact
1	Outage is surgical — only VLAN 40 ↔ VLAN 10 blocked	Looks like a targeted attack. But also consistent with a misconfigured rule.	Supports A and C equally
2	RetailLink firmware update at 9:30 AM	RED HERRING. Update was successful. Terminals are online. Problem is network, not terminals.	Supports then eliminates B
3	SSH scanning from 185.220.101.34 at 2 AM	Real scanning. But all attempts FAILED. No access gained. Motivated Kelley to write the rule.	Supports A initially. Actually explains the motive for C.
4	RetailLink says "unusual API queries" on their portal	RED HERRING. RetailLink's cloud problem, not NCIA's. Adds noise.	Supports A (falsely)
5	Firewall rule CM-2026-0087 at 09:45	2 minutes before outage. Source=any, Dest=10.1.40.0/24, Action=DENY. Position 3.	**CONFIRMS C. ELIMINATES A and B.**

6	Post-change verification not completed	Kelley was called to a meeting. Never tested. Process failure.	Explains why C wasn't caught immediately
7	Self-approval policy for emergency changes	No peer review. No second set of eyes. Systemic failure.	Root cause of C

3. FACILITATOR PERFORMANCE NOTES

Managing the Red Herrings

The SSH scanning and the RetailLink firmware update are REAL events. They happened. They're in the evidence packet. They are designed to pull the team toward Theory A and Theory B. Do NOT discourage the team from investigating them — let them chase the leads. The learning happens when they realize they were wrong. If you steer them away from the red herrings too early, they never experience the confirmation bias lesson.

The Firewall Rule Is the Key

The entire puzzle collapses once IT reads the actual rule in Exhibit B of the Evidence Packet. Source Zone = any, Source Address = any, Destination = 10.1.40.0/24, Action = DENY. If IT reads this early and identifies the errors, the puzzle is solved quickly — reward that. If they haven't read the rule by 0:40, inject I-05 delivers it directly.

The Jordan Kelley Debate

This is the emotional core of the exercise. Kelley is the IT Manager — he's senior, trusted, competent. He made a mistake that cost the airport an hour of retail revenue and triggered airline delays. Some students will want to fire him. Others will defend him. Both sides have merit. The best outcome is when the team recognizes that the SYSTEM allowed the mistake: self-approval, no peer review, no automated validation, no post-change testing. If Kelley hadn't made this error, someone else would have eventually. The facilitator should push BOTH sides: "So you'd fire your IT Manager for a typo?" and "So you'd give him a pass after he crashed your retail network for an hour?"

4. PACING GUIDE

Phase	Clock	Duration	Notes
0: Briefing	0:00 – 0:10	10 min	Present all three theories equally. Do NOT hint at the answer. Let IT study the Evidence Packet.
1: Chase the Theories	0:10 – 0:40	30 min	Let them chase red herrings. RetailLink call (I-02) partially eliminates B. SIEM analysis (I-03) supports A but also introduces the timeline leading to C. Media pressure (I-04) forces PIO to act under uncertainty.
2: Evidence Converges	0:40 – 1:10	30 min	I-05 is the aha moment. The actual rule is read. Theory C confirmed. Then: fix the immediate problem, manage airlines, manage media. The truth is embarrassing but necessary.
3: The Reckoning	1:10 – 1:40	30 min	Root cause analysis. The Kelley debate. Process improvement. This phase is discussion-heavy — let the room argue.
4: Debrief	1:40 – 2:00	20 min	3-Up / 3-Down. Focus on: confirmation bias, change management, and the tension between accountability and blame.

5. EVALUATION & GRADING RUBRIC

Metric	Assessment Criteria
Metric 1: Diagnostic Accuracy (30 Points)	**Fail:** Team declared a cyberattack without confirming. Never read the firewall rule. **Pass:** Team eventually identified Theory C as correct after working through the evidence. **Excellence:** IT identified the firewall rule errors independently from the Evidence Packet, correlated the 09:45 change with the 09:47 outage, and eliminated A and B with specific evidence.
Metric 2: Operational Management (25 Points)	**Fail:** Team focused entirely on investigation. Tenants, airlines, and passengers were ignored. **Pass:** Ops coordinated cash-only procedures and communicated with tenants and airlines. **Excellence:** Ops had cash-only signage deployed within 10 minutes, directed passengers to ATMs, coordinated with airline ops on kiosk workarounds, and gave tenants a restoration timeline.
Metric 3: Crisis Comms (20 Points)	**Fail:** PIO confirmed a cyberattack prematurely, or gave "no comment" to all inquiries. **Pass:** PIO issued a holding statement that didn't confirm or deny attack. **Excellence:** PIO had differentiated statements pre-drafted for all three scenarios, issued accurate correction once cause was confirmed, and proactively managed the media narrative.
Metric 4: Process Improvement (25 Points)	**Fail:** Team focused on blaming Kelley. Didn't address systemic issues. **Pass:** Team identified the self-approval policy and lack of peer review as contributing factors. **Excellence:** Team produced a comprehensive improvement plan: mandatory peer review, automated rule validation, post-change verification checklist, staging environment, and a nuanced accountability approach for Kelley that balances consequences with culture.

6. HOT WASH GUIDE

- **Confirmation Bias:** "You had real SSH scanning, a real vendor update, and a real firewall change. Two of those were red herrings. Which theory did you chase first — and was it because of evidence or instinct?"
- **The 2-Minute Gap:** "The rule was applied at 9:45. The outage started at 9:47. That's a 2-minute correlation. How long did it take you to make that connection?"

• **Self-Approval:** "Kelley approved his own change under the emergency threat mitigation policy. Should ANY firewall change be self-approved? What about at 2 AM when nobody else is available?"

• **Post-Change Verification:** "Kelley didn't test after applying the rule. If he had pinged one POS terminal from the Server VLAN, he'd have caught it in 30 seconds. Should post-change verification be mandatory and automated?"

• **The Kelley Question:** "In aviation, we have just culture — we don't punish honest mistakes, but we hold people accountable for reckless behavior. Was Kelley's mistake honest or reckless? Where's the line?"

• **The Communication Trap:** "If PIO had said 'cyberattack' at noon and you found out it was a typo at 12:30, could you undo that headline? What does premature disclosure cost?"

END OF CONTROLLER HANDBOOK