



AIRPORT CYBER RESILIENCE SIMULATOR

VERSION 2 · PLAYER & FACILITATOR GUIDE

How to play, how to think, and what the experience is designed to teach — a companion for visitors at the kiosk and for the facilitators running the stand.



THE MESSAGE

What this simulation is about

The Airport Cyber Resilience Simulator is not a quiz with a right answer — it is a decision game about consequence. You take the seat of an airport's incident commander during a live cyber attack and discover, in ninety seconds, that every option on the table costs something. The goal is to make the trade-offs felt, not just explained.

Five ideas it is designed to land:

Idea	What the player experiences
1 · Small door, big house	A single unglamorous entry point — a USB stick, a default password, a phishing email — cascades across critical infrastructure.
2 · There are no free wins	Every mitigation trades security against operational capacity and cash. Doing nothing also has a price, ticking up every second.
3 · Consequence scales	Heathrow and a regional airport face the same attack but very different financial and regulatory exposure.
4 · Comms is response	How you talk to the public moves the loss line as sharply as any technical control.
5 · Regulation is real	Each node maps to an NCSC CAF objective and a UK Cyber Security and Resilience Bill duty — the fines are not invented.

THE APPROACH — ONE ROUND, ABOUT 2-3 MINUTES

How to play

1 Set the stakes — choose an airport

Pick the airport on the configuration screen. This is a difficulty dial: a Tier-1 hub bleeds cash fast and carries maximum statutory fines; a regional airport is a gentler first game. Everything downstream scales to this choice.

2 Choose a threat and start

Select one of the nine playbooks and press START SIMULATION. Use the 5-second countdown to orient: find the glowing ingress node and trace the dotted links leading away from it — that is the likely blast radius.

3 Read the board

At zero, the method-of-ingress icon pulses over the entry node, then it turns red. Red particles race down the links to the next target on a timer. Watch the sidebar: the financial odometer starts climbing white → amber → red, and the Live Incident Log narrates every event.

4 Decide under pressure

Tap a compromised node and pick a mitigation. You cannot save everything — the spread timer is running, so choose which node to defend and how. The Regulatory Insights tab tells you why a node matters.

5 Brief the media and the regulators

Two duties run in parallel. The Crisis Communications panel opens a 15-second proactive window — handle it, silence is expensive. At the same time the Notify CAA and Notify DfT buttons light amber if this incident type carries a statutory reporting duty; press the ones that apply. Failing to notify a required regulator adds an enforcement penalty at the end.

6 Reach containment and close out

Keep isolating or patching until the spread can no longer advance. Once no new node is compromised for five seconds the simulation ends with ATTACK CONTAINED and the clock and financial bleed freeze. Read the final numbers, then press RESET to CONFIG for the next player.

HOW TO THINK ABOUT THE TRADE-OFFS

Strategy

There is no single winning line, but there is skilful play. Strong players triage: they decide what to sacrifice before the spread forces their hand.

THE MITIGATION DECISION MATRIX

Move	Reach for it when...	What you are buying
Isolate Node	The next hop is a crown jewel (identity, border, power, ATC) and you cannot afford the spread.	Stops spread dead. Accept 0% capacity and maximum operational bleed on that node.
Reduce / Throttle	You want to keep partial service running and buy time to think or to patch elsewhere.	Slows the spread 80% and holds 40% capacity — a hedge, not a cure.
Stop Attack (Patch)	You can start the 5-second patch early enough to beat the attack to the next node — you will see it closing in as the patch counts down.	Restores the node to normal — but £50k is spent whether or not you win the race.

Protect the data-sensitive nodes first

Identity Store, Passenger Services, Frequent Flyer DB, Border Control API and Ticketing DB trigger huge one-off regulatory fines the instant they are breached — scaled by your airport. If one of these is the next hop, isolating or patching upstream before it falls is usually worth the operational hit.

Win the comms game every time

Releasing a proactive statement in the first 15 seconds halves the reputational multiplier ($\times 0.5$), which slows the entire financial bleed. Miss it and answer the flashing phone/email to hold the baseline ($\times 1.0$). Ignore the barrage and a blackout triples it ($\times 3.0$) — the single most expensive mistake available.

Mind the clock — and the tempo

Every scenario has its own spread speed, and it shifts slightly each run. Fast attacks — ransomware, signal spoofing, the perimeter breach — usually outrun a patch entirely, so isolate instead. Slower, stealthier ones give a patch time to land. Throttling also multiplies the remaining delay $\times 5$, which can turn a patch you would have lost into one you win. Read the tempo before you commit £50k to a patch.

Notify the right regulator — the duty matches the breach

Attacks that touch air traffic, runway or aircraft systems must be reported to the Civil Aviation Authority; disruption to critical transport infrastructure and passenger data goes to the Department for Transport; the most serious incidents require both. The sidebar buttons light up only for the duties this scenario actually triggers — press them, or take a per-regulator enforcement penalty at the end. The deck below shows who to call for each playbook.

NINE PLAYBOOKS, NINE LESSONS

The scenario deck

Each playbook is a self-contained talking point. Rotate them to keep a stand fresh and to show how varied the attack surface really is.

#	Scenario	Ingress	Notify	The lesson it teaches
1	The OT Gridlock	USB drive	DfT	Removable media walks straight past the perimeter into OT.
2	The Silent Choke	Default password	CAA + DfT	Cheap smart-building IoT bridges into safety-critical systems.
3	The Third-Party Siphon	Phishing email	DfT	Your suppliers' security is your security.
4	The Rogue Insider	Rogue smartphone	CAA	Stolen legitimate access defeats the perimeter entirely.
5	The Blind Spot	VPN breach	CAA + DfT	An unmanaged path can reach kinetic, life-safety systems.

#	Scenario	Ingress	Notify	The lesson it teaches
6	The Information Hijack	Password crack	DfT	Public-facing displays and PA are an integrity and panic risk.
7	The Perimeter Ghost	Rogue router	DfT	Physical and cyber security are one problem, not two.
8	The Data Hemorrhage	Cloud leak	CAA + DfT	A misconfiguration can leak PII at scale and stack fines.
9	The Grid Overload	Malware update	DfT	Energy and EV infrastructure is now part of the attack surface.

WHAT GOOD LOOKS LIKE

Reading the result

The best possible ending is ATTACK CONTAINED — you stopped the spread before it ran its course. Whether contained or fully spread, the debrief lives in a handful of numbers and the story behind them. Use these as discussion prompts:

Metric	A good outcome	Debrief question
Outcome	ATTACK CONTAINED before full spread	Which mitigation finally halted it — and could it have come sooner?
Total Financial Loss	As low as the situation allowed	What drove it — bleed, fines, comms failure, or a missed notification?
Security Integrity	Kept as high as possible	Which nodes were sacrificed, and were they the right ones?
Operational Capacity	Traded knowingly, not accidentally	Did isolating for safety visibly close the runway or stop bags?
Reputation multiplier	×0.5 (proactive)	Was the public told early, or did the story get away?
Statutory notifications	CAA / DfT discharged as required	Did you match the notification to the type of breach?

FACILITATOR NOTES

Running the stand

- Session length: one round is 2-3 minutes. Let a visitor lose badly once — the trade-off lands harder than a clean win.
- Audio: set it on the configuration screen to match the hall. The countdown ticks and ingress thud are strong attention-grabbers on a busy floor.
- Kiosk mode: full-screen the browser (F11). After 90 seconds idle the app returns to the attract loop by itself.
- Reset ritual: press RESET TO CONFIG between visitors so each person sets their own airport and owns the outcome.
- Great opening question: "You have one attack incoming and you cannot save every system — what do you protect first?"

Ultimately the simulator argues one thing: resilience is not the absence of incidents, it is the quality of the decisions you make during one.