SOFEMA
AVIATION SERVICES

CYBER RISK

AVIATION INTERFACE CHALLENGES

Anecdotal Case-notes for group discussion.

PRESENTED BY:
Rustom D. Sutaria

CYBER SECURITY FOCUS

01. YOUR TASK

02. 2022 - SWISSPORT RANSOMWARE

03. 2022 - JEPPESEN (BOEING) CYBER INCIDENT

04. 2023 - FEAM AERO RANSOMWARE CLAIM

04. 2023 - BOEING PARTS & DISTRIBUTION CYBER INCIDENT

05. 2024 - TECHNICAL DEPENDENCE FRAGILITY

06. 2025 - HAWAIIAN AIRLINES CYBER INCIDENT

CYBER SECURITY FOCUS

07. 2025 - HAWAIIAN AIRLINES CYBER INCIDENT

08. 2025 - QANTAS CUSTOMER-DATA BREACH

09. 2025 - COLLINS AEROSPACE (RTX) CHECK-IN/BOARDING SYSTEMS RANSOMWARE

10. 2026 - REGULATORY CLOCK AND DOMINANT ATTACK PATTERNS

YOUR TASK

This workbook uses real-world aviation cyber incidents from 2022 - 2026, to explore how disruptions propagate through commercial air transport operations and maintenance/MRO interfaces.

You will review each short anecdote, identify the affected operational and maintenance touchpoints, and map likely failure modes (data loss, access disruption, supplier concentration, degraded-mode working).

For each case, you will capture safety performance impacts and compliance implications, then propose practical controls, contingencies, and assurance checks. Use the prompts to drive discussion, compare scenarios, and translate lessons into actions you can apply in your own organisation.

2022

SWISSPORT RANSOMWARE

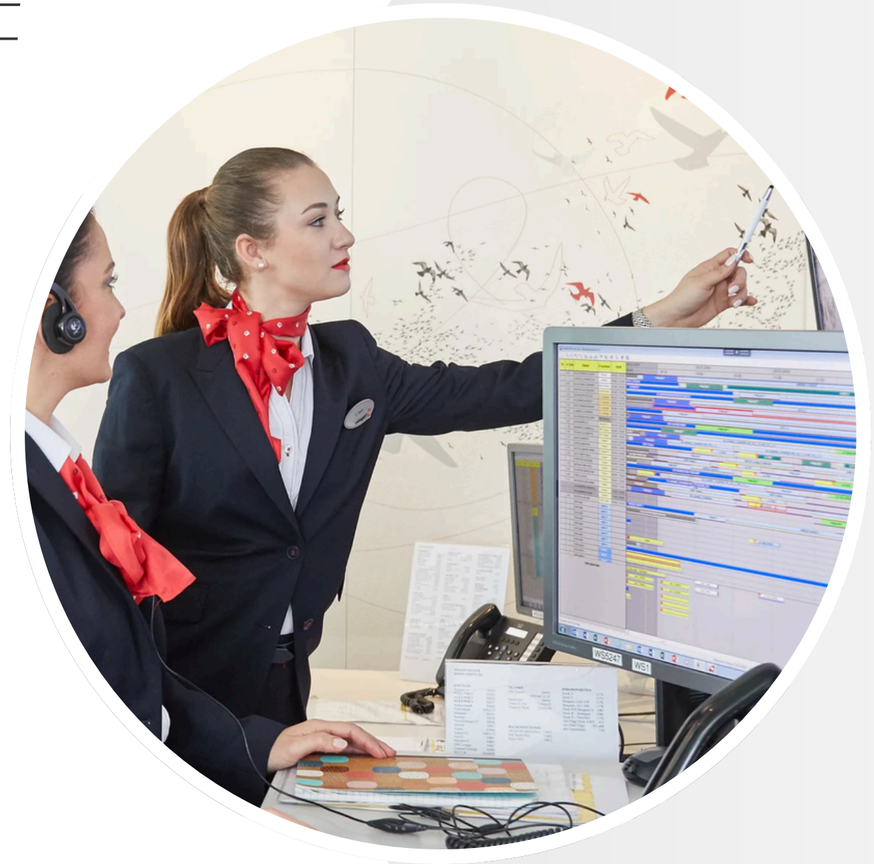
Ground handling + cargo interface

What happened: Swissport, a major ground handler, was hit by ransomware and took systems offline while containing the incident.

Operational impact lens: Partner IT disruption drives airport-level degraded operations (manual processing, queues, missed connections, delay propagation).

Maintenance/MRO lens: Turnaround degradation creates schedule shock; rotations collapse, night-stops change, and line maintenance volatility increases.

Discussion prompt: Who “owns” the operational risk when on-time performance depends on third-party cyber resilience?



2022

JEPPESEN (BOEING) CYBER INCIDENT

Disruption of flight-planning products.

What happened: Jeppesen services were impacted by a cyber incident, disrupting certain flight-planning products/services.

Operational impact lens: Dispatch becomes data-limited; planning, routing, and nav-data distribution constraints can become operational hazards.

Maintenance/MRO lens: Irregular ops (re-routes, altered alternates, MEL utilisation changes) shifting maintenance planning assumptions and deferred defect trajectories.

Discussion prompt: Where is your “minimum viable dispatch” line if flight &/or maintenance planning tooling is degraded?

2023

FEAM AERO RANSOMWARE CLAIM

MRO / line-maintenance footprint

What happened: FEAM Aero was publicly reported/claimed as a ransomware victim.

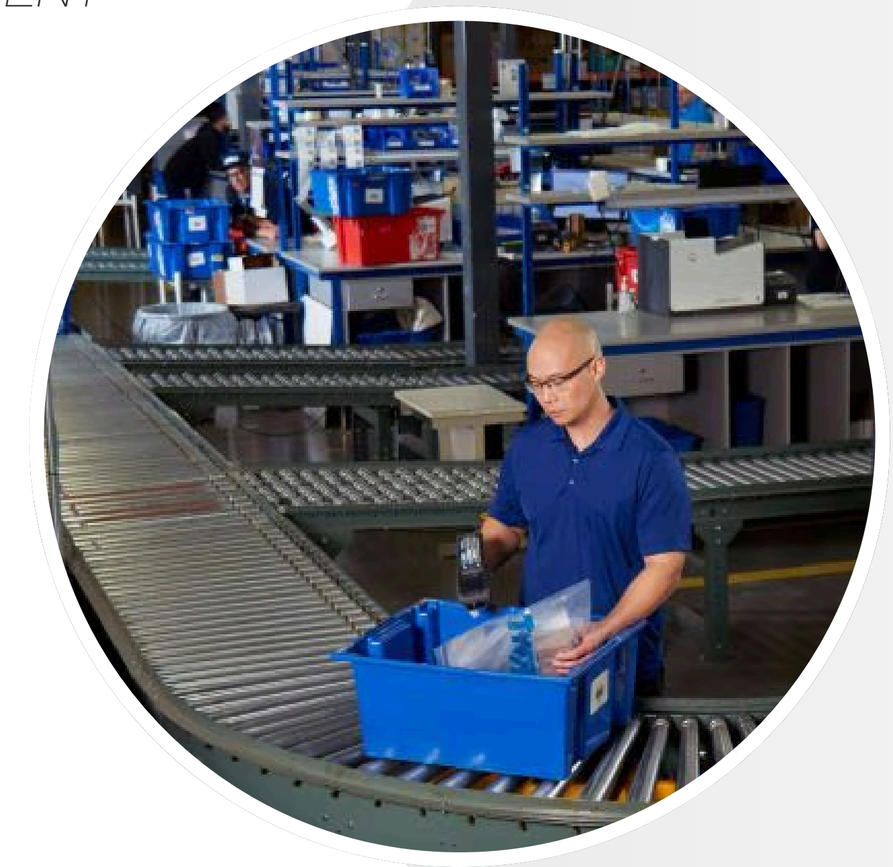
Operational impact lens: Multi-station MRO disruption can slow return-to-service cadence for customer operators.

Maintenance/MRO lens: IT unavailability hits workpacks, task cards, parts ordering, engineering records, and access control; record integrity becomes a central risk.

Discussion prompt: What do you do if the MRO cannot access the maintenance system-of-record for 48 hours?

2023

BOEING PARTS & DISTRIBUTION CYBER INCIDENT



Supply-chain shock

What happened: Boeing reported a cyber incident impacting parts and distribution business elements.

Operational impact lens: Less visible than a flight-ops outage, but can quietly increase delays via spares constraints.

Maintenance/MRO lens: Spares delays extend AOG time and force logistics workarounds; alternative sourcing and quarantine controls matter.

Discussion prompt: How does cyber resilience show up inside your spares KPIs (fill-rate, backorder age, AOG hours, etc.)?

2024

TECHNICAL DEPENDENCE FRAGILITY

What could happen: Industry commentary highlights that aviation's interconnected, legacy-heavy tech stack can suffer major disruption regardless of the presence of a confirmed cyberattack.

Operational impact lens: Contingency plans must handle both cyber and non-cyber technology failures similarly (degraded modes, manual fallbacks, prioritisation).

Maintenance/MRO lens: Digitisation (eTech logs, e-signatures, connected tooling) demands credible offline *'work-as-done'* procedures and reconciliation.

Discussion prompt: Which safety-critical maintenance tasks cannot tolerate loss of digital identity/access services?

2025

HAWAIIAN AIRLINES CYBER INCIDENT

airline internal IT disruption

What happened: Hawaiian Airlines reported a cybersecurity incident disrupting some IT systems while stating flights operated safely.

Operational impact lens: Separating IT service impact from safety impact is essential under pressure - especially public messaging and regulator coordination.

Maintenance/MRO lens: Maintenance control, tech records access, defect control, and release paperwork can be impaired even when flying continues.

Discussion prompt: Which maintenance decisions become riskier when data integrity/availability is uncertain?

Click Here to read the article

2025

WESTJET CYBERSECURITY INCIDENT

app + internal systems; later notification

What happened: WestJet disclosed an incident affecting internal systems and its app; later reporting indicated some passenger data exposure.

Operational impact lens: Customer-facing disruptions add comms load; peaks in support demand elevate social-engineering risk.

Maintenance/MRO lens: Helpdesk strain and credential workflows can spill into contractor/vendor accounts used by maintenance and engineering support.

Discussion prompt: How do you harden contractor access during an incident when support channels are overloaded?

Click Here to read the article

2025

QANTAS CUSTOMER-DATA BREACH

Via third-party contact-centre platform

What happened: Qantas confirmed a cyberattack potentially exposing customer data via a third-party contact-centre platform.

Operational impact lens: Third-party platform compromise demonstrates concentration risk beyond airline core systems.

Maintenance/MRO lens: The pattern transfers directly to MRO ecosystems (hosted tools, engineering services, training platforms, parts marketplaces).

Discussion prompt: How do you assure your critical suppliers' security without inheriting their entire risk?

Click Here to read the article

2025

COLLINS AEROSPACE (RTX) CHECK-IN/BOARDING SYSTEMS RANSOMWARE

Vendor → multi-airport disruption

What happened: A cyberattack on Collins Aerospace disrupted check-in/boarding systems at multiple major European airports.

Operational impact lens: Shared-service concentration risk—one supplier outage ripples across hubs causing manual processing, delays, cancellations.

Maintenance/MRO lens: Mass irregular ops amplifies line maintenance volatility and increases documentation error risk under time pressure.

Discussion prompt: What is your policy for maintenance documentation quality during mass disruption + manual operations?

2026

REGULATORY CLOCK AND DOMINANT ATTACK PATTERNS

What will be happening: Ongoing reporting highlights ransomware + credential theft/social engineering as dominant patterns; multiple EU information-security risk requirements take effect in 2026.

Your Operational Context: Compliance deadlines drive governance, reporting, and assurance expectations across operators and critical suppliers.

Your AMO/CAMO context:
Part-145/Continuing Airworthiness organisations must evidence risk management for ICT dependencies, supplier access, and data integrity.

Discussion prompt: How will you demonstrate both compliance impact and safety performance impact for the same cyber control?

SOFEMA
AVIATION SERVICES

SECURE AVIATION
PROTECT EVERY FLIGHT

Hardening your systems, train your people, and verify your controls before disruption affects your flights.