OT-ISAC

OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

In the spirit of community-driven collaboration, OT-ISAC encourages Members and Partners to share information that strengthens collective defence and situational awareness.

OT-ISAC members requiring direct assistance may submit a request through the OT-ISAC Member Portal. Our team will provide support through the member submission and RFI process.

KEEPING AIRPORTS MOVING

Cyber Dependencies, Third-Party Concentration and Operational Resilience in the Airport Ecosystem

PUBLIC SECTOR INTELLIGENCE REPORT

August 2026

> **Purpose**
> A concise public assessment of airport cyber dependencies, shared-service concentration and the practical measures that preserve safe, orderly operations when digital systems become unavailable or untrusted.

Prepared by OT-ISAC

Based exclusively on publicly available information. No member-derived incident reporting, sensitive asset data or non-public indicators are included.

EXECUTIVE BRIEF

Airport resilience is an ecosystem-continuity problem

Cyber defence matters when it preserves safe, orderly airport operations during loss of trust, visibility or shared digital services.

● Why this matters

Airports are systems of systems. Passenger processing, baggage, operational data, identity, physical access, facilities, communications and partner platforms must work together at high tempo.

The most probable cyber consequence is not compromise of an aircraft. It is reduced airport capacity: slower check-in and boarding, baggage disruption, loss of passenger information, constrained gates or stands, and intensive manual coordination.

● Who should use this report

✓ Airport operators and authorities
✓ Airlines and ground handlers
✓ Airport IT, OT and security teams
✓ National CERTs and aviation regulators
✓ Technology providers and system integrators
✓ Operations, resilience and crisis teams

Use it to decide

✓ Which shared services could create multi-party impact
✓ How much throughput fallback processes can sustain
✓ Which supplier access paths require immediate control
✓ How recovery data will be verified and reconciled

Multi-Airport
A single common-use provider incident disrupted passenger and baggage processing at several European airports in September 2025.

3,600+
Volunteer hours used during the first ten days of the 2024 SEA Airport outage to support passengers and manual information flows.

Feb 2026
Regulation (EU) 2023/203 became applicable on 22 February 2026, following the first major Part-IS milestone in October 2025.

Key judgements

HIGH	The most credible route to airport disruption is compromise of shared IT, passenger-processing, identity or operational-support services rather than direct manipulation of safety-critical aviation systems.
HIGH	Third-party concentration can convert one provider incident into simultaneous impact across multiple airports, airlines and handling organisations.
HIGH	Manual fallback can preserve operations, but normally at materially reduced throughput and only when staffing, data, communications and procedures have been exercised.
MODERATE-HIGH	Enterprise compromise can affect airport operations through displays, baggage interfaces, access control, gate and stand coordination, parking, facilities and partner communications.
MODERATE	Direct malicious manipulation of safety-relevant airport OT remains less commonly evidenced in public incidents, but potential consequence warrants strict separation, monitoring and recovery controls.

Bottom line
Airport resilience is the ability to contain one digital failure, preserve a shared operational picture, continue safely at a defined reduced capacity and recover without propagating untrusted data.

THREAT PICTURE

What is driving airport-sector cyber risk?

Shared platforms, complex ownership boundaries, extensive outsourcing and high-volume operations create concentrated dependencies.

Threat pattern	Typical access	Operational relevance	Assessment
Shared platform or supplier compromise	Provider intrusion, privileged access, software or cloud service disruption	Check-in, boarding, baggage and common-use services may fail across multiple stakeholders.	High concentration risk.
Ransomware or enterprise intrusion	Phishing, stolen credentials, exposed services or third parties	Displays, kiosks, identity, Wi-Fi, websites, parking, communications and support services may become unavailable.	Common; impact varies.
DDoS and hacktivism	Public websites, apps, APIs and external services	Passenger information and public confidence may be affected; direct operational impact is usually limited unless dependencies are poorly separated.	Likely during geopolitical tension.
Remote-access or credential abuse	Vendor portals, support accounts, VPNs, jump hosts or unmanaged endpoints	May provide a route to baggage, facilities, access-control or airport-operations systems.	High relevance where access is broad.

Evidence boundaries

CONFIRMED
Public incidents have disabled or degraded check-in, boarding, baggage, displays, websites, Wi-Fi, ticketing and parking services.

ASSESSED
Shared identity, operational databases, resource-management, access-control and facilities dependencies can create wider cascades when architectures or recovery processes are weak.

NOT ESTABLISHED
Terminal disruption does not by itself demonstrate compromise of aircraft flight controls, air traffic control, navigation safety or deliberate unsafe aircraft movement.

Classify the incident before describing the impact

SAFETY-RELEVANT AVIATION SYSTEM COMPROMISE	Evidence shows unauthorised change to a system or data whose integrity or availability can affect aviation safety. This requires specific technical and operational evidence.
AIRPORT OPERATIONAL DISRUPTION	Airport capacity, passenger or baggage flow, access, facilities, resource coordination or airside support is degraded, even where core safety systems remain available.
PASSENGER-PROCESSING / ENTERPRISE DISRUPTION	Corporate, public-facing or common-use services are affected. Operational impact must be assessed through dependencies and fallback capability.

Analytical discipline
A cyber incident at an airport is not automatically an aviation-safety compromise. Describe the affected service, ownership boundary, operational consequence and recovery evidence separately.

OPERATIONAL IMPACT

How digital service loss becomes operational disruption

Airport consequence is shaped by dependency design, peak demand, staffing, partner coordination and the throughput of fallback processes.

1	2	3	4	5
ENTRY	**SHARED ACCESS**	**SERVICE LOSS**	**OPERATIONAL EFFECT**	**RESPONSE**
Supplier compromise, phishing, exposed service, stolen credential or ransomware	Common-use platform, identity, cloud service, remote management or network trust	Check-in, boarding, baggage, displays, gate/stand data, access or facilities support	Queues, missed connections, baggage delay, manual coordination and capacity reduction	Containment, alternate systems, degraded operation, passenger communication and staged recovery

Two high-probability pathways

THIRD-PARTY CONCENTRATION PATH
Provider compromise > common passenger or baggage service unavailable > multiple airports and airlines affected > manual processing, delays and cancellations.

AIRPORT ENTERPRISE-TO-OPERATIONS PATH
Airport compromise > identity, communications, displays, parking or support services unavailable > staff workarounds > reduced throughput and prolonged recovery.

Critical dependencies to map

PASSENGER FLOW Check-in, self-service kiosks, boarding, common-use platforms and passenger data

OPERATIONAL DATA Airport operational database, flight information displays, gates, stands and resource allocation

BAGGAGE Reconciliation, sortation, tracking, screening interfaces and handling coordination

IDENTITY & ACCESS Workforce identity, privileged accounts, vendor access, badges and physical access control

FACILITIES OT Building systems, power, runway lighting, boarding bridges, fuel controls and environmental systems

CONNECTIVITY Campus networks, cloud services, radio, mobile, APIs and partner data exchanges

PARTNERS Airlines, handlers, border agencies, security providers, air navigation and emergency services

PUBLIC COMMUNICATION Websites, apps, signage, social channels, help desks and disruption messaging

Operational resilience target

ISOLATE	COORDINATE	OPERATE	RECOVER
Disconnect affected paths without causing unnecessary loss of safe airport services.	Maintain one trusted operational picture across airport, airlines, handlers and agencies.	Continue safely at a predefined reduced capacity using alternate or manual processes.	Reconnect only after security validation, data reconciliation and operational testing.

CASE STUDIES

Three transferable lessons from public incidents

The value is not the incident count. It is what each case reveals about shared services, reduced throughput and coordinated recovery.

01

Collins Aerospace common-use systems incident - September 2025

CONFIRMED FACTS A cyber incident affecting Collins Aerospace disrupted check-in, boarding and baggage-related services at several European airports. Affected airports used manual and alternative procedures; Brussels Airport reported flight cancellations, while BER progressively restored its central handling service.

TRANSFERABLE LESSON A compromise at one external provider can create simultaneous multi-airport impact without evidence of compromise at each affected airport. Contracted recovery, alternate processing and cross-party coordination are operational controls.

EVIDENCE BOUNDARY *Public reporting established passenger-processing disruption, not compromise of aircraft, air traffic control or flight-safety systems.*

02

Port of Seattle / SEA Airport ransomware - August 2024

CONFIRMED FACTS The Port of Seattle attributed the incident to Rhysida ransomware. Isolation actions and encryption hindered baggage, check-in kiosks, ticketing, Wi-Fi, passenger displays, the website, app and reserved parking. The Port reported that the majority of affected services returned within a week, while restoration of some external and internal services continued longer.

TRANSFERABLE LESSON Manual operations impose a substantial human and information burden. SEA used handwritten signs, third-party information sources and almost 500 volunteers who contributed more than 3,600 hours in the first ten days.

EVIDENCE BOUNDARY *The Port stated that travel remained safe. The incident demonstrates airport-service disruption and data compromise, not confirmed safety-system manipulation.*

03

Kuala Lumpur International Airport cyber incident - March 2025

CONFIRMED FACTS Malaysia Airports and NACSA reported a cybersecurity threat affecting certain KLIA computer systems. Authorities launched an investigation and stated that flight operations and passenger processing continued normally. A ransom demand was publicly reported by Malaysia's Prime Minister.

TRANSFERABLE LESSON Operational continuity is an important outcome, not evidence that the incident was insignificant. Architectural separation, rapid escalation and coordinated monitoring are transferable controls; public reporting did not establish which specific controls preserved continuity at KLIA.

EVIDENCE BOUNDARY *Public disclosures did not identify affected system functions in detail and did not establish direct OT or aviation-safety impact. Later actor claims should not be treated as confirmed attribution without official validation.*

Shared lesson

Operational consequence depends on concentration, architectural separation, fallback throughput, trusted data, staffing and the speed at which multiple organisations can coordinate.

What the cases do not show

They do not demonstrate that airport disruption normally involves aircraft systems, air traffic control or unsafe flight operations. These outcomes require separate evidence and should not be inferred from queues, cancellations or terminal outages.

PRIORITISATION AND DETECTION

Prioritise access, criticality and blast radius - not CVSS alone

The most urgent risks combine operational importance, a viable access path and the ability to affect multiple airlines, handlers, terminals or airports.

	LOWER ACCESSIBILITY	HIGHER ACCESSIBILITY
HIGH CRITICALITY	**PROTECT AND MONITOR** Local baggage or facilities controllers, runway-lighting components, fuel controls or access-control infrastructure with tightly controlled pathways.	**IMMEDIATE ACTION** Externally reachable operational portals, broad supplier access, shared identity, common-use passenger platforms, cloud operational data or remote gateways into baggage and facilities systems.
LOWER CRITICALITY	**ROUTINE MANAGEMENT** Isolated support systems with limited integration, low operational consequence and tested recovery.	**SECURE PROMPTLY** Public websites, apps, parking, retail or support services. Assess credential reuse, data sensitivity and hidden integrations into higher-value systems.

High-value detection opportunities

• New or unusual privileged access to common-use, operational-data or supplier platforms	• Repeated authentication failures followed by success from new locations or devices
• Remote supplier sessions outside approved work orders or maintenance windows	• Unexpected changes to MFA, identity federation, service accounts or recovery contacts
• Simultaneous loss or mismatch of flight, gate, stand, baggage or display data	• Configuration or logic changes in baggage, boarding bridge, facilities or runway-lighting systems
• Abnormal badge-policy changes, access-control events or mass credential activation	• Large data exports from passenger, employee, parking or contractor systems
• Outages spanning multiple terminals, airlines or airports that share a provider	• Recovery log gaps, unverified software builds, data reconciliation failures or premature reconnection

Detection principle

Monitor changes to shared operational truth and the access paths that allow one account, provider or platform to affect multiple stakeholders. Alerting should connect cyber events to capacity and continuity indicators.

RESILIENCE ROADMAP

Priority actions for airport ecosystems

Sequence improvements around dependency visibility, controlled third-party access, tested degraded operations and coordinated recovery.

0-30 DAYS	30-90 DAYS	3-12 MONTHS
• Map every externally hosted, common-use and supplier-managed operational service.	• Map dependencies among passenger processing, baggage, operational data, identity, access and facilities.	• Segment critical airport OT and operational services from enterprise and public-facing environments.
• Identify and remove dormant, shared or excessive third-party accounts; require MFA where feasible.	• Run a multi-party exercise with airport, airlines, handlers, agencies and key technology providers.	• Implement privileged-access management and monitored support paths for suppliers and integrators.
• Define minimum viable airport operations and acceptable reduced throughput for each terminal.	• Centralise logs for identity, supplier access, administration and critical operational services.	• Test degraded operations during realistic peak volume and minimum staffing conditions.
• Confirm offline contact lists, escalation paths and alternate passenger communication methods.	• Define secure recovery, data reconciliation and controlled reconnection procedures.	• Establish baseline monitoring for baggage, facilities, boarding bridges, runway lighting and access control.
• Verify emergency isolation contacts and incident-notification obligations for priority suppliers.	• Set contractual recovery objectives, evidence requirements, backup expectations and emergency support.	• Assess supplier concentration, substitution options and exit or continuity plans for critical shared services.

Five-minute readiness pulse

This is a decision prompt, not a maturity score. A "No" to any of the first six questions warrants priority attention.

☐ Can you identify the business owner, technical owner, supplier and fallback for every critical shared service?	☐ Can you revoke or isolate all non-essential supplier access quickly without losing safe operations?
☐ Can airlines and handlers process passengers and bags at reduced capacity, and for how long?	☐ Can partners maintain one trusted operational picture if email, collaboration or central dashboards fail?
☐ Are offline procedures, contact lists, gate/stand plans and passenger messages current and accessible?	☐ Can staff independently verify flight, gate, baggage, identity and access data before acting on it?
☐ Does recovery reconcile transactions and operational data before systems are reconnected?	☐ Has degraded operation been tested at peak demand, with realistic staffing and vulnerable passengers considered?

Operational test

An airport ecosystem should be able to isolate one common service, continue safely at a declared capacity limit, maintain coherent passenger and partner communications, and reconcile data before normal operations resume.

APAC OUTLOOK AND SOURCES

Implications for APAC airport operators

APAC hubs combine rapid digital growth, complex partner ecosystems and significant national dependence on reliable air connectivity.

Regional considerations

- APAC includes globally connected hubs alongside smaller airports with uneven cyber resourcing and supplier leverage.
- Extensive outsourcing to airlines, ground handlers, integrators and cloud or common-use providers creates complex accountability boundaries.
- Rapid terminal expansion and digitalisation can connect modern passenger platforms to long-lived facilities and operational systems.
- Cross-border dependencies complicate notification, evidence preservation, regulatory coordination and recovery support.
- Multilingual communications, seasonal peaks, transfer passengers and cargo operations increase the consequence of inconsistent disruption messaging.
- Singapore and other highly connected economies depend on reliable air hubs for trade, essential supplies and regional connectivity.

12-18 month outlook

VERY LIKELY Ransomware, credential theft and data extortion will continue against airport operators, airlines, handlers and technology providers.

LIKELY Supplier and cloud-service incidents will produce multi-tenant disruption and difficult questions over recovery evidence and responsibility.

LIKELY DDoS and hacktivist activity will target visible airport and airline services during geopolitical tension, usually with greater reputational than safety effect.

POSSIBLE Cyber and hybrid events involving GNSS interference, drones or communications disruption will increase, but should be assessed separately from airport-network compromise.

MODERATE CONFIDENCE Regulatory and safety-linked information-security requirements are expected to improve governance, while implementation maturity and supplier visibility are likely to remain uneven across APAC.

Regional priority

Treat supplier assurance, multi-party exercises and fallback throughput as regional resilience issues - not solely as internal airport IT controls.

Method and limitations

Information current to 4 August 2026. The report uses public sources and separates confirmed facts from OT-ISAC assessment. Public reporting may omit technical detail or understate impact. Likelihood and confidence terms are qualitative analytical judgements.

Selected references

[1] FIRST, Traffic Light Protocol (TLP) Version 2.0.

[2] ICAO, Aviation Cybersecurity Strategy.

[3] ENISA, NIS360 2026, aviation subsector assessment, 28 May 2026.

[4] ENISA, Threat Landscape: Transport Sector, 2023 (dataset: Jan 2021-Oct 2022).

[5] UK NCSC, Statement: Incident Impacting Collins Aerospace, 20 Sep 2025.

[6] Brussels Airport, September 2025 Traffic Results, 10 Oct 2025.

[7] Berlin Brandenburg Airport, Update on Cyber Attack on Service Provider, 2 Oct 2025.

[8] Port of Seattle, Port Cyberattack Archive, updated 2024-2025.

[9] Port of Seattle, Employees Pitched in during the SEA Cyberattack, 4 Dec 2024.

[10] Bernama, KLIA Cybersecurity Threat - Operations Unaffected, 25 Mar 2025.

[11] EASA, Easy Access Rules for Information Security, Dec 2025.

[12] TSA, Cybersecurity Requirements for Airport and Aircraft Operators, 7 Mar 2023.

[13] ICAO APAC / JCAB, Measures and Policies on Civil Aviation Cybersecurity, 2025.

[14] ACI World / Changi Airport Group, Cybersecurity by Design, 2 Apr 2024.

[15] Singapore Ministry of Transport, Aviation, accessed 4 Aug 2026.