Open Sky, Open Threats

A Case Study of the Kuala Lumpur International Airport Ransomware Incident (March 2025)

Group Members

Adjei Ernest — Registration No.: 000623556 — ULB

Volonterio Luca — Registration No.: 000622673 — ULB

Hussaini Mohmmad Qasim — Registration No.: 000623362 — ULB

ELEC-H550 - Embedded System Security

Professor Jan Tobias Mühlberg

Université Libre de Bruxelles

Academic Year 2025–2026

Abstract

This report analyzes the March 2025 ransomware incident at Kuala Lumpur International Airport (KLIA) to understand how converged IT and Operational Technology (OT) architectures create specific vulnerabilities in modern aviation infrastructure. As airports integrate IT and OT to handle millions of transactions daily, their attack surface expands and previously peripheral vendor platforms become critical dependencies. Using Level-1 Data Flow Diagrams and the STRIDE threat modeling framework, the report reconstructs the passenger-processing subsystem and identifies likely failure modes in the Airport Operational Database (AODB), Common-Use Passenger Processing Systems (CUPPS), and Baggage Handling Systems (BHS). Our analysis suggests that weakly segmented vendor remote-access channels and shared identity infrastructure enabled lateral movement into passenger-processing systems, resulting in a cascading denial of service: flight safety remained intact, but check-in and baggage handling were severely degraded, forcing a reversion to manual "whiteboard" operations. Evaluating the incident against Malaysia's Cyber Security Act 2024 and the Personal Data Protection Act (PDPA) indicates that, while regulatory frameworks for critical infrastructure exist, practical enforcement and assurance for third-party embedded systems are insufficient. The report concludes with recommendations on strengthening vendor governance, deploying immutable and regularly tested backups, and enhancing IT/OT segmentation for KLIA and comparable airports.

Contributions

This report was developed collaboratively by all group members. **Adjei Ernest** contributed the system overview of airport passenger-processing under normal operating conditions and developed the Data Flow Diagram (DFD), including key data flows and trust-boundary definition. **Hussaini Mohmmad Qasim** led the impact assessment, including evaluation of operational disruption, financial implications, and potential data-protection exposure. **Volonterio Luca** conducted the threat modeling and security analysis, including the application of the STRIDE framework and the development of the STRIDE-based threat assessment matrix. All members contributed to literature review, writing, editing, and final validation of the report.

Contents

1 Introduction

Modern airports have evolved from simple transport hubs into highly integrated cyber–physical ecosystems. Compared with other public infrastructures such as hospitals or railway systems, airports occupy a uniquely attractive position in the cyber-threat landscape due to their operational complexity, rich data holdings, and immediate public exposure. Aviation operations rely on tightly coupled IT and OT systems that cover passenger processing, baggage handling, air-traffic coordination, payment services, and third-party vendor platforms, such that compromise of a single component can rapidly propagate across organizational and national boundaries.

Reflecting this exposure, the aviation sector experienced a reported 600% year-on-year increase in ransomware attacks between January 2024 and April 2025 [1]. These environments also aggregate high-value data, including biometric identifiers, travel histories, and sensitive operational information, which is easily monetizable or exploitable for espionage. Unlike healthcare or rail networks, where disruptions may remain partially localized, outages at major airports become visible within minutes, affecting large passenger populations and triggering cascading economic impacts across airlines, logistics, and tourism. This sustained threat pressure is shown in the scale of defensive investment, with the global aviation cybersecurity market estimated at USD 5.32 billion in 2025, while the sector's role as critical national infrastructure also attracts geopolitically motivated actors seeking strategic intelligence or symbolic disruption [1].

Kuala Lumpur International Airport (KLIA), Malaysia's primary aviation gateway and one of Southeast Asia's busiest hubs, exemplifies this complexity. Handling an average of 130,000 passengers daily and connecting to more than 1,200 weekly flights across 60 international destinations, KLIA functions as a high-density data ecosystem reliant on continuous digital interconnectivity. Such scale and technological dependence make it a high-value target for cyber adversaries seeking to disrupt operations, extort ransom payments, or test the resilience of national infrastructure.

In March 2025, KLIA experienced a major ransomware attack that disabled critical passenger-processing systems and forced a temporary reversion to manual operations. The incident underscored the paradox of modern aviation infrastructure: while open and interconnected networks enable operational efficiency and data sharing, they also expand the potential attack surface susceptible to exploitation.

2 Objectives

The primary goal of this report is to analyze the KLIA ransomware incident to understand how cyber-physical convergence creates specific vulnerabilities in the aviation sector. Specifically, the objectives are:

1. **Problem Statement:** To address the vulnerability of converged IT/OT systems in high-value aviation targets where third-party dependencies create hidden risks.

2. **Technical Analysis:** To model the passenger-processing subsystem and identify specific failure modes using standard threat modeling frameworks.

3. **Impact Assessment:** To verify what can be proven from open data regarding the operational, financial, and data-protection impacts of the attack.

4. **Regulatory Context:** To evaluate whether existing frameworks (Act 854, PDPA) are sufficient to ensure vendor resilience and operational continuity.

5. **Incident Control and Recovery:** To analyse, based on observable outcomes and standard critical-infrastructure practices, how operational control was lost and subsequently re-established in the absence of full forensic disclosure.

3 Literature Review

This section surveys the existing architectural standards and literature relating to airport operational systems to establish the baseline environment.

3.1 General Airport Architecture

As illustrated in Figure 1, a modern international airport functions as a highly integrated *cyber–physical ecosystem*. At a structural level, the airport can be understood as a multi-layered environment consisting:

- **Landside**: Comprises passenger access points, terminal operations, public information services, and airline interfaces.

- **Airside**: Covering aircraft movement, ground handling, maintenance, and navigation aids, which rely on tightly controlled OT networks.

- **Enterprise IT**: Hosting corporate, administrative, and analytical functions, also central databases.

- **Operational Technology**: Responsible for physical processes and control systems, including SCADA, PLCs, and safety instrumentation.

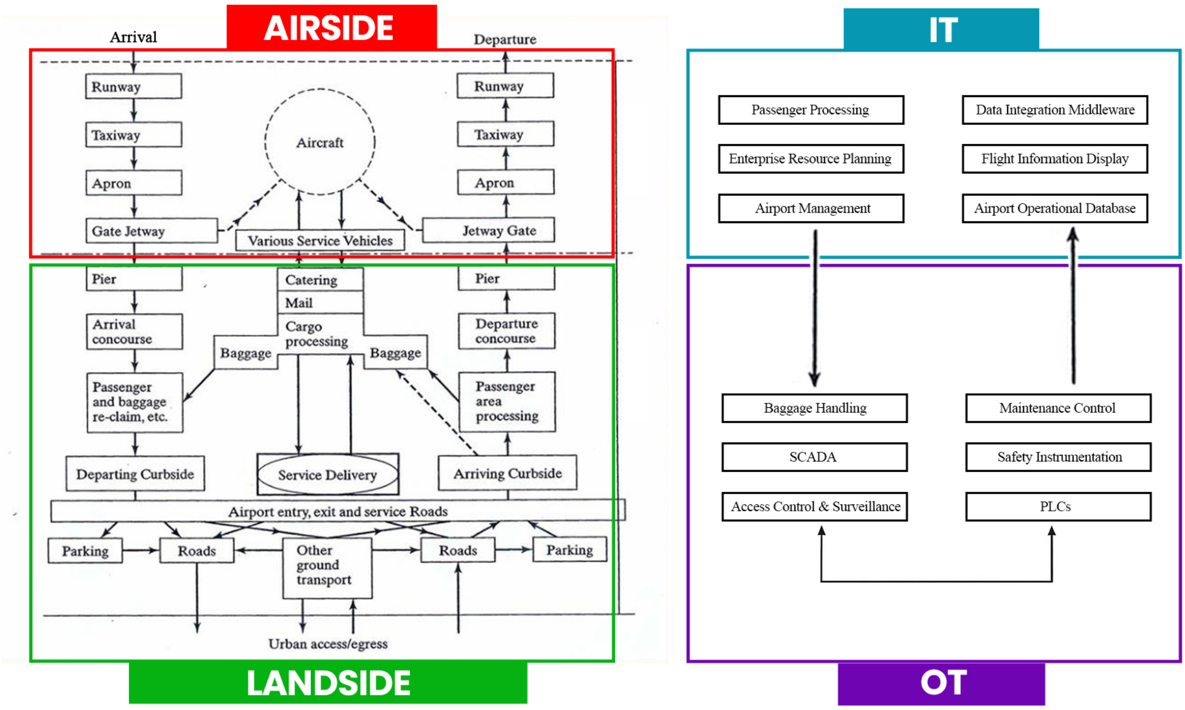


Figure 1: General airport architecture showing the integration of IT and OT layers.

3.2 Passenger-Processing Subsystem Architecture

The core of the analysis focuses on the passenger-processing subsystem. The literature defines the following functional components as critical for operations:

Table 1: Functional overview of passenger-processing subsystem components

Component	Primary Function
AODB (Airport Operational Database)	Central data spine integrating flight schedules and resource statuses. Publishes operational updates via APIs.
FIDS (Flight Info Display)	Displays live arrival/departure info; receives updates from AODB.
CUPPS (Common-Use Processing)	Shared platform for airline check-in; connects to airline DCS and issues bag tags.
BHS (Baggage Handling)	Automates baggage routing via PLCs. Consumes Bag Source Messages (BSM) from CUPPS.

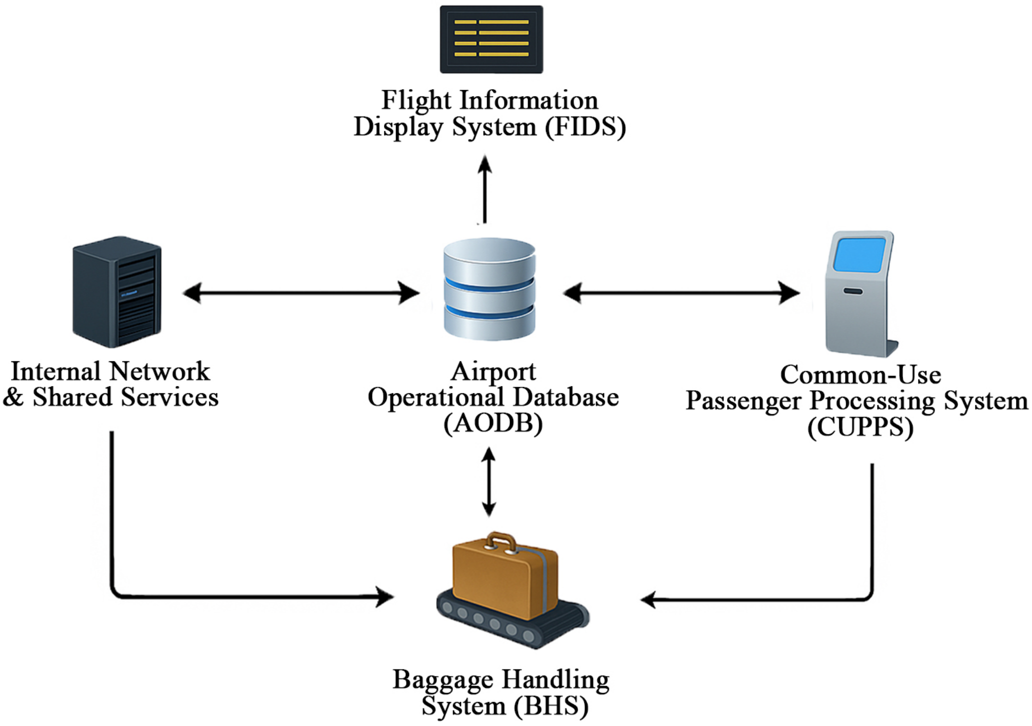

Flight Information Display System (FIDS)
Internal Network & Shared Services
Airport Operational Database (AODB)
Common-Use Passenger Processing System (CUPPS)
Baggage Handling System (BHS)

Figure 2: Overview of the passenger-processing subsystem.

4 Methods

To reconstruct the incident and analyze the security posture of KLIA, this report utilizes two primary methodological tools: Data Flow Diagrams (DFD) and the STRIDE threat modeling framework.

4.1 Data Flow Analysis

We employ Level-1 Data Flow Diagrams to map the end-to-end flow of information between the AODB, CUPPS, FIDS, and external entities. The diagram was developed using publicly available airport architecture standards and ICAO aviation cybersecurity guidance describing typical passenger-processing workflows and system interactions [8, 9]. A Level-1 abstraction was selected to capture system-level data exchanges and trust relationships while avoiding implementation-specific details that are not publicly disclosed, with the scope limited to passenger-processing functions relevant to the incident. Crucially, this approach defines the trust boundary separating airport-managed IT/OT systems from untrusted external entities, such as passengers, public networks, and external airline systems.

4.2 STRIDE Threat Modeling

The STRIDE framework [20, 19] is applied to the defined architecture to categorize potential threats. This ensures a comprehensive analysis of the attack surface:

- **S**poofing of Identity
- **T**ampering with Data
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Service
- **E**levation of Privilege

Where public sources describe concrete facts, these are treated as observed elements. Where sources are silent, threat scenarios are **assumed** based on common Qilin ransomware tactics and typical airport IT/OT environments.

4.3 Methodological Use of Generative AI

In the preparation of this report, our team utilized Generative AI tools to support our research, drafting, and formatting processes. We view AI as a productivity tool that enhanced the clarity and presentation of our findings, while the core analysis and technical verification remained the responsibility of the group members.
Our usage of AI tools focused on the following key areas:

- **Brainstorming and Ideation**: We used AI during the initial planning phase to explore different angles of the Kuala Lumpur International Airport (KLIA) incident. This helped us brainstorm potential threat scenarios relevant to embedded systems and identify key architectural components (such as the AODB and CUPPS) that required investigation.
- **Resource Gathering**: AI assisted us in identifying some relevant information.
- **Language Refinement and Polishing**: As English is not our first language, we used AI to review our drafts for grammatical correctness, spelling, and sentence flow.
- **Formatting and Typesetting**: Finally, AI was used to generate the necessary LaTeX code to format this report.

5 Implementation and Execution of Analysis

This section details the specific challenges identified in the airport's procedures and the execution of the threat model against the baseline architecture.

5.1 Trust Boundary Definition

This trust boundary is defined according to administrative control and security governance rather than physical location, in line with established threat modeling practice [19, 18]. Systems within the boundary are operated by the airport authority under a shared security policy, identity management infrastructure, and monitoring regime, which justifies their treatment as a single trusted domain for analytical purposes. In contrast, external entities including passengers, public web portals, airline departure control systems, and vendor remote access operate under independent security controls and trust assumptions and are therefore modeled as untrusted. Explicitly delineating this boundary highlights the interfaces where authentication, authorization, and segmentation failures may enable lateral movement into airport information technology and operational technology systems, which is central to the subsequent STRIDE analysis [20, 19].

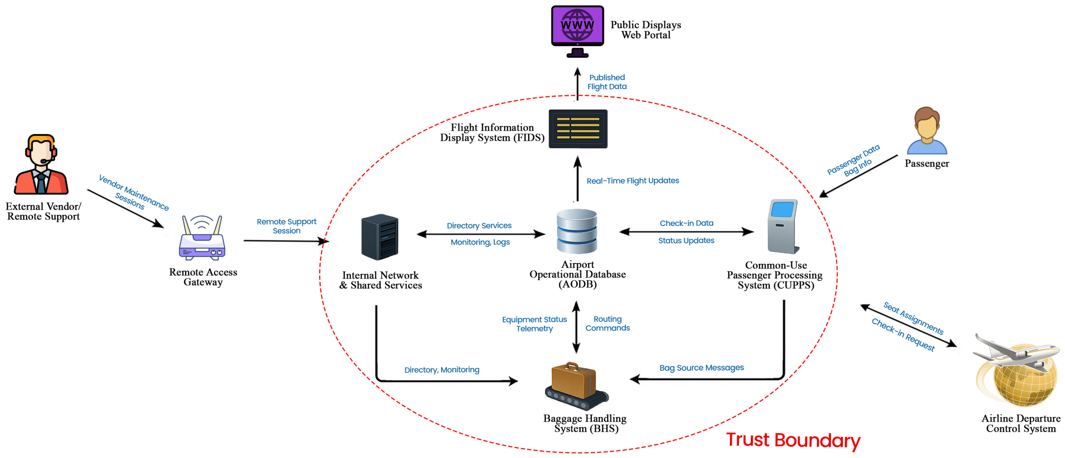


Figure 3: Combined Data Flow Diagram (DFD) and Trust-Boundary View.

5.2 Vulnerabilities and Failure Dynamics

The analysis identified critical dependencies that acted as failure points during the execution of the attack. KLIA relies on an interconnected ecosystem in which mission-critical services depend on external vendor platforms, as highlighted by post-incident analyses and industry commentary [2, 7, 10]. More broadly, ICAO guidance recognises that aviation environments rely on highly interconnected systems and third-party dependencies, which increases exposure when governance and segmentation controls are weak [8, 9].

5.2.1 Technical Attack Narrative

The reconstruction of the attack path, based on publicly available analysis and typical ransomware TTP, reveals a clear progression of compromise across the airport's critical systems [2, 7, 10]:

Initial Access via Vendor Remote Access Gateway The attack likely exploited weakly governed vendor credentials to gain access through the Remote Access Gateway. Vendor remote access is a standard feature of airport environments, enabling third-party vendors to provide support for CUPPS, baggage handling systems, and other critical components [9]. However, if vendor credentials lack multi-factor authentication (MFA) or are insufficiently monitored, they become a high-value initial access vector [2, 7, 3]. In the KLIA case, the porous boundary between vendor support channels and core IT infrastructure allowed the attacker to establish a foothold within the airport's operational domain [2, 10].

Lateral Movement via Shared Identity Infrastructure Once initial access was gained, the attacker leveraged shared identity infrastructure to move laterally from the IT zone (where the Remote Access Gateway resides, along with CUPPS and AODB) into the OT zone hosting the Baggage Handling System (BHS). The "Trust Boundary" between these zones, while conceptually defined, was effectively porous due to several technical factors, consistent with common failure modes in converged IT/OT environments [8, 9]:

- Federated access mechanisms linking CUPPS, AODB, and BHS supervisory nodes to shared authentication pools (e.g., LDAP, Kerberos, or vendor-managed single sign-on) [3, 10];
- Service accounts with excessive privilege scopes permitting automated data flow between zones (a typical propagation enabler in ransomware campaigns) [20, 21];
- Insufficient network segmentation or unidirectional gateway enforcement, allowing data and access tokens to traverse back across the boundary [9, 37].

These conditions meant that compromise of a single account or service token in the IT zone directly enabled access to OT-managed systems. The attacker, having established a foothold via vendor credentials, was able to enumerate and impersonate privileged service accounts used by the AODB and CUPPS to communicate with BHS controllers, which aligns with STRIDE *Elevation of Privilege* and common ransomware operator tradecraft [20, 21, 22].

Payload Execution and Cascading Failures Once privileged access was obtained across both IT and OT zones, the attacker deployed ransomware targeting the AODB—the central data spine of the airport's operational ecosystem (Table 1). While open reporting does not confirm AODB encryption explicitly, mapping disruption to the AODB is a plausible architecture-based inference that explains multi-system degradation under ransomware conditions [2, 25, 27]. The AODB is not merely a database; it is the authoritative source of truth for:

- Flight schedules, aircraft movements, and gate assignments (consumed by FIDS, ground handlers, and ATC coordination);
- Baggage routing rules and handling instructions (consumed by BHS via published APIs and message queues);
- Passenger and resource allocation data (consumed by CUPPS for check-in and load balancing).

Encryption of the AODB resulted in an immediate and cascading *Denial of Service* across the passenger-processing chain, consistent with public accounts describing disruption to check-in, baggage processes, and information systems [25, 2, 27]:

1. **FIDS Outage**: Flight information displays became unable to fetch live data, forcing reliance on manual boards [2, 25].
2. **CUPPS Degradation**: Check-in systems could not issue accurate bag tags or confirm baggage routing instructions, making electronic baggage tracking impossible [25, 2].
3. **BHS Failure**: Baggage sorting equipment, dependent on BSM messages and routing rules from CUPPS, could no longer route bags to correct destinations and had to shut down processing [2, 10].
4. **Manual Fallback**: Airlines and ground handlers were forced to issue handwritten bag tags, manually sort baggage, and use whiteboard-based gate assignments, reverting to procedures not routinely exercised and unsuitable for high-volume operations [2, 25, 10].

This cascade occurred because the AODB outage was not contained by architectural segmentation; instead, it propagated immediately to dependent systems, illustrating a known fragility in converged IT/OT environments when central coordination services are compromised [9, 37].

This reconstructed attack path provides the technical basis for the STRIDE-based interpretation and comparative risk discussion developed in Section 7 [20, 19].

6 Results

This section presents the findings of the investigation, including the confirmed timeline, the operational status, and the results of the STRIDE threat matrix.

6.1 Incident Timeline

From open sources, the detection and response are confirmed, while the technical impact and duration remain partially unclear. As shown in Figure 4, available reporting indicates an initial disruption beginning on 23 March 2025 followed by partial restoration and attribution reports by 27 March 2025.

Table 2: Confirmed and reported events in the KLIA ransomware incident timeline.

Date	Event	Validity
23 March 2025	KLIA detected a cybersecurity threat affecting certain systems. MAHB launched an investigation.	Confirmed
23 March 2025	Group-IB reported a 10-hour critical system outage.	Reported (analyst)
25 March 2025	PM Anwar Ibrahim confirmed hackers demanded USD 10 million.	Confirmed

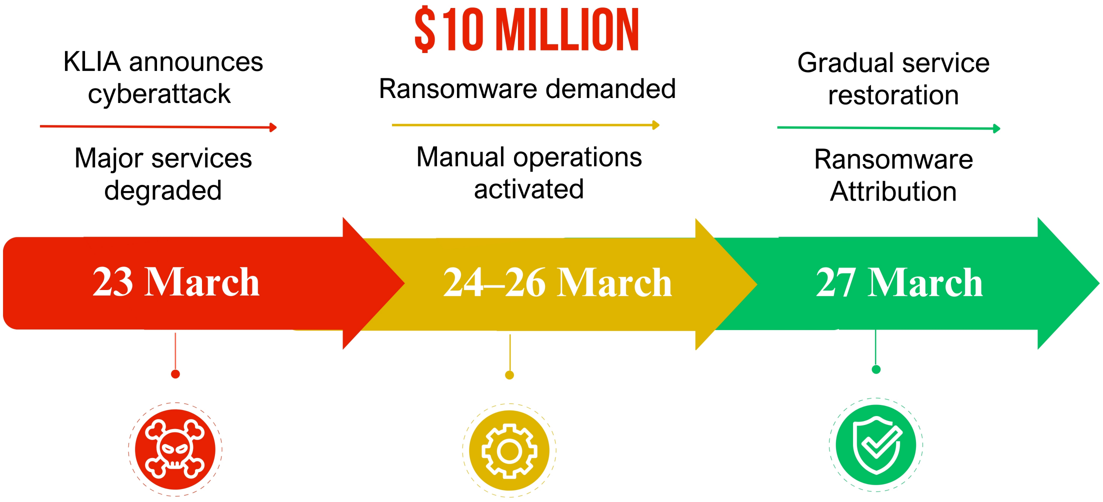


Figure 4: Visual incident timeline for the KLIA ransomware attack. Adapted from public reporting. Source: [28, 27].

6.2 Operational and Data Findings

Public data confirms that MAHB detected a threat and informed NACSA [28]. While MAHB stated flight operations were not disrupted, analyst reports describe a disruption of check-in and baggage-related systems lasting approximately 10 hours [27]. This discrepancy affects the confidence of downstream impact estimation because the disruption may have impacted embedded passenger-processing and baggage-handling workflows without directly grounding flights.

6.3 Containment, Recovery, and Re-establishment of Control

Although detailed technical remediation steps were not publicly disclosed, available statements and the observed restoration of airport services indicate that Malaysia Airports Holdings Berhad (MAHB) ultimately regained control of the affected infrastructure through a combination of containment, isolation, and controlled system recovery [28, 5]. As with many incidents affecting

Table 3: Potential data exposure results based on the system architecture and typical airport passenger-processing workflows.

System	Typical data handled	Exposure level
Check-in / CUPPS	Passenger names, passports	Possible
Flight Info Display	Schedules (no PII)	Unlikely
Baggage Controllers	Bag tags, flight numbers	Possible
Admin / HR Servers	Employee/Vendor data	Likely

critical infrastructure, recovery focused first on operational continuity and safety, followed by progressive restoration of digital services.

Containment and Isolation Following detection of the incident, affected systems were likely isolated to prevent further lateral propagation. In converged IT/OT environments, this typically involves disabling external remote access pathways, revoking or resetting potentially compromised credentials, and segmenting impacted network zones to stabilise unaffected systems [9, 37]. Public confirmation that flight safety systems remained operational suggests that containment measures successfully prevented escalation into airside safety-critical domains [28].

Operational Continuity via Manual Control During the containment phase, the airport reverted to manual operational procedures, including handwritten baggage tags, manual passenger processing, and ad-hoc information displays. While inefficient, these procedures allowed the airport to maintain basic functionality while digital systems were unavailable [2, 25]. This step effectively decoupled physical operations from compromised digital control layers, buying time for technical recovery.

System Restoration and Revalidation Regaining control of the infrastructure would have required restoring core systems from known-good states. In ransomware incidents where payment is refused, this typically involves reimaging affected hosts, restoring databases from backups where available, and re-establishing trust in identity and access management systems through credential resets and privilege review [21, 22]. Analyst reporting indicating a finite disruption window of approximately 10 hours suggests that partial system functionality was restored relatively quickly, even if full forensic validation and hardening continued beyond the initial recovery period [27].

Coordination and Oversight The involvement of Malaysia's National Cyber Security Agency (NACSA) indicates that recovery occurred under national critical-infrastructure incident management processes [5]. Such coordination typically includes technical assistance, situational assessment, and validation that restored systems can be safely returned to service. However, the absence of publicly released post-incident technical details limits external assessment of the depth of system cleansing and assurance achieved prior to resuming normal operations.

Overall, the restoration of operations demonstrates that control was re-established primarily through isolation, manual fallback, and staged system recovery rather than rapid digital remediation alone. This reinforces the importance of pre-planned continuity procedures and trusted recovery mechanisms in environments where full forensic certainty cannot be achieved immediately.

6.4 STRIDE Threat Matrix Findings

The STRIDE model highlights how vendor access, identity management, segmentation weaknesses, and limited forensic visibility interact to shape the KLIA incident. Table 4 provides a concise overview of the main attack vectors, affected components, and high-level impacts.

Table 4: STRIDE Threat Matrix for KLIA Passenger Processing System

STRIDE	Attack Vector	Primary Components	Impact (summary)
S	Vendor credential misuse	Remote access gateway, AODB, CUPPS	Plausible spoofing of third-party access; initial entry vector.
T	Ransomware deployment	AODB, application servers	Encryption and/or disruption of core operational data.
R	Limited forensic visibility / possible anti-forensics	Logs, IdPs, security tooling	Incomplete reconstruction of attack chain due to absent or undisclosed logs.
I	Suspected data exfiltration	PII repositories, admin systems	Large-scale data theft plausible.
D	Service disruption	Passenger-processing chain (CUPPS, BHS, FIDS)	Cascading operational outage.
E	Privilege escalation	Shared identity infrastructure	Broad cross-system access via privileged/service accounts; likely enabled lateral movement.

7 Discussion

This section interprets the results, returning to the problem statement to discuss the financial implications and the regulatory context of the incident.

7.1 Interpretation of STRIDE Findings

Taken together, the STRIDE results summarise how the most plausible threats emerge from the intersection of the reconstructed KLIA architecture and the limited open-source evidence on the incident. For *Spoofing* (S), post-incident analyses consistently emphasise vendor remote access channels and third-party accounts, but no public source describes a concrete credential-theft or impersonation technique. Modelling spoofing via compromised vendor credentials is therefore consistent with common ransomware tradecraft in complex enterprise environments and KLIA's reliance on remote support, yet remains an inferred rather than a confirmed mechanism [2, 7, 10]. The absence of authentication artefacts in public disclosures further limits external verification of the initial access vector.

For *Tampering* (T), official and analyst reports agree that ransomware was deployed and that "critical systems" and data became unavailable, but they do not specify which exact databases, configuration stores, or backup repositories were encrypted. Mapping this impact to the AODB and CUPPS/BHS data paths is therefore an architecture-based inference that explains the observed service degradation, not a proven forensic statement about specific tables or storage layers [27, 25]. In ransomware campaigns, deliberate suppression or destruction of system telemetry can further obscure the precise scope of tampering, particularly in environments with fragmented logging across IT and OT domains [21, 22].

The *Repudiation* (R) category is especially salient in this incident. Official statements and media coverage provide only coarse-grained and partially inconsistent timelines, with no disclosure of detailed endpoint, authentication, or network logs [28, 5]. While the absence of such artefacts cannot be taken as evidence of deliberate log erasure, it is consistent with common ransomware operator practices aimed at reducing post-incident traceability, including log clearing, use of legitimate administrative tools, and blending malicious actions into normal operational activity [21, 24]. From a structural perspective, this highlights repudiation as a systemic risk arising from distributed ownership of logs across airport operators and third-party vendors, rather than a single technical failure.

For *Information Disclosure* (I), several threat-intelligence and media sources report substantial data exfiltration and cite approximate volumes on the order of terabytes, but the exact composition of those datasets and the specific systems involved are not documented. Associating potential disclosure with passenger-processing and administrative data stores is therefore reasonable from an architectural viewpoint but must be presented as unverified, particularly given the lack of forensic artefacts confirming data staging or transfer paths [27, 13].

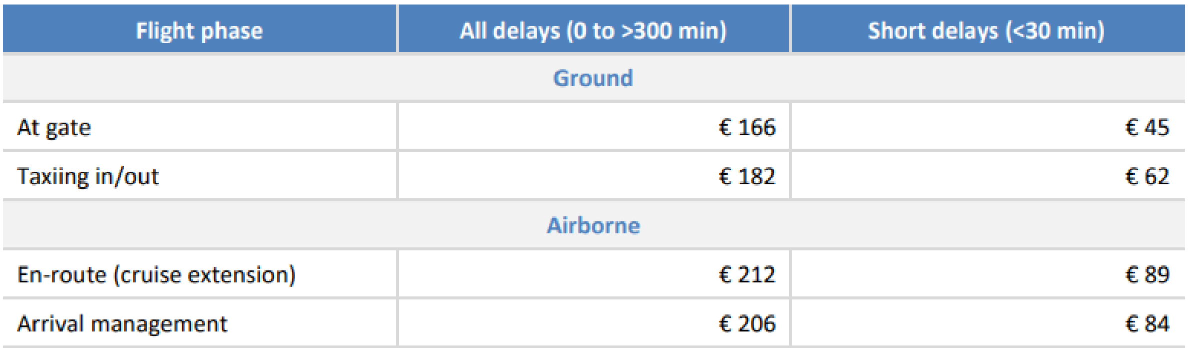
By contrast, *Denial of Service* (D) is the most strongly supported category. Multiple accounts describe prolonged disruption, reversion to manual check-in and baggage handling, and degraded display systems, even if the precise duration and quantified operational impact vary between official and analyst narratives [25, 2, 26]. Interpreting this disruption through the reconstructed architecture clarifies why "manual fallbacks" became the only viable option: once a central operational database such as the AODB is unavailable, the airport's digital ecosystem loses its authoritative "source of truth" for coordination, forcing reliance on organisational workarounds until central services are restored.

Finally, *Elevation of Privilege* (E) is implied by the breadth and speed of cross-system impact from an assumed vendor entry point. While account-level forensic confirmation is unavailable, rapid reach across CUPPS, AODB, and BHS supervisory domains strongly suggests compromise of privileged or service accounts trusted across segments via shared identity infrastructure. This inference aligns with known ransomware operator behaviour, where elevated credentials both enable lateral propagation and support anti-forensic actions such as disabling security tooling or suppressing logs, but it remains an analytical conclusion rather than a verified attribution for KLIA [21, 22, 23].

7.2 Interpretation of Operational and Financial Impact

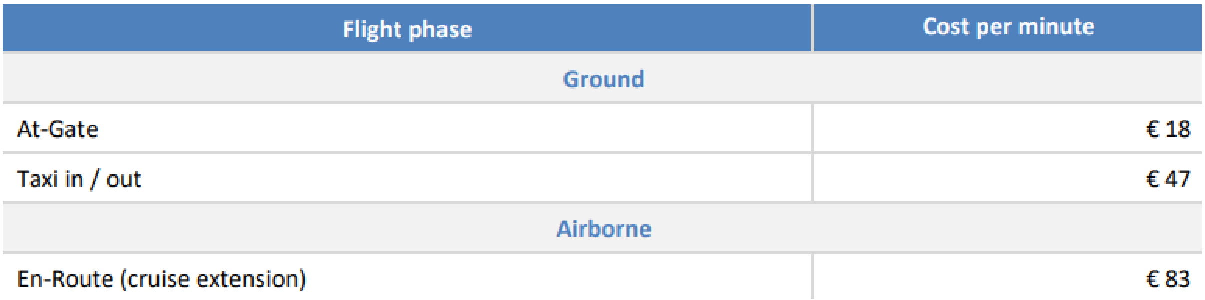
The contradiction between official statements (minimal disruption) and analyst reports (approximately 10-hour outage) highlights the difficulty in assessing cyber impacts on embedded systems at airports. However, using EUROCONTROL standard cost inputs [29] as a reference, we can interpret the potential operational and financial consequences of degraded passenger-processing services.

As shown in Table 6, even short disruptions leading to gate or taxi delays create measurable operational costs. In particular, at-gate delays are estimated at 18 € per minute on average, and taxi in/out delays at 47 € per minute. Table 5 further highlights that delay cost can increase significantly when network effects are considered, reinforcing that the financial pressure from such incidents can be immediate, even if flights are not formally cancelled.



Flight phase	All delays (0 to >300 min)	Short delays (<30 min)
Ground		
At gate	€ 166	€ 45
Taxiing in/out	€ 182	€ 62
Airborne		
En-route (cruise extension)	€ 212	€ 89
Arrival management	€ 206	€ 84

Table 5: EUROCONTROL tactical delay cost (incl. reactionary delay / network effect) per minute, by flight phase. Source: [29].



Flight phase	Cost per minute
Ground	
At-Gate	€ 18
Taxi in / out	€ 47
Airborne	
En-Route (cruise extension)	€ 83

Table 6: EUROCONTROL strategic delay cost per minute, by flight phase. Source: [29].

7.3 Ransom Demand and Payment Stance

Public reporting indicates that the attackers demanded a ransom of around USD 10 million [28]. Based on public statements by the Malaysian Prime Minister reported in open sources, the Malaysian government publicly refused to pay the ransom [28]. Publicly available information does not confirm any payment being made, and this report therefore treats payment as unverified.

7.4 Regulatory and Security Framework Analysis

The incident was analyzed against the Cyber Security Act 2024 (Act 854) and the Personal Data Protection Act 2010 (PDPA), with a focus on whether observed incident handling behaviour aligns with legal obligations and where operational gaps remain [31, 30].

- **Act 854 relevance and alignment:** Act 854 regulates National Critical Information Infrastructure (NCII) and defines governance and incident reporting expectations for critical infrastructure operators [31]. In this incident, MAHB's notification of NACSA and public confirmation of an active cyber threat indicate alignment with the incident escalation and coordination intent of the Act [28].

- **Act 854 gaps for embedded/OT environments:** While the legal framework supports reporting and governance, public evidence remains limited regarding proactive enforcement and continuous assurance measures. In particular, there is no clear public indication of OT-focused vendor audits, continuous monitoring requirements, or systematic assurance for network-connected embedded systems involved in passenger processing and baggage workflows. This suggests a gap between high-level statutory requirements and the practical verification of resilience for operational technology and embedded subsystems.

- **PDPA relevance and operational implications:** PDPA requires personal data to be protected against unauthorised access, disclosure, alteration, or misuse [30]. Since vendors and airport IT operators process personal data through check-in and CUPPS environments, this implies a need for enforceable technical controls to reduce exposure and prevent unauthorised access during system degradation.

- **Link from law to technical recommendations:** The incident supports a compliance-driven interpretation of security controls: vendor privileged access to airport systems should be continuously governed and verified. For example, enforcing PAM (Privileged Access Management) and MFA for vendor accounts operationalises PDPA requirements by reducing the likelihood of credential-based compromise and limiting exposure of PII, while also supporting Act 854-aligned risk management by limiting propagation into interconnected airport systems [31, 30].

7.5 Comparative Critical Infrastructure Risk

A key question raised by the KLIA case is why airports represent an especially effective target for ransomware operators compared with other critical sectors. While many infrastructures have high societal value, airports exhibit a combination of rapid operational coupling and strong network effects that translate technical disruption into immediate, measurable economic pressure.

Using EUROCONTROL standard cost inputs as a comparative anchor, even routine delay externalities are non-trivial: at-gate delays are estimated at approximately 18 € per minute and taxi in/out delays at approximately 47 € per minute (Tables 6 and 5) [29]. These values become strategically relevant in ransomware contexts because airports amplify disruption through *reactionary delay* and interconnected schedules: a disruption window of roughly 10 hours, as reported by analyst sources [27], can generate compounding delays across inbound and outbound rotations, crew duty limits, baggage logistics, and downstream connections.

Compared with hospitals or railways, airports face unusually strong *global bottleneck* dynamics. Hospitals may degrade into local contingency modes (triage prioritisation and temporary diversion), and rail networks can sometimes reroute or isolate affected lines; however, a major hub airport functions as a high-density coordination node in a tightly synchronised, international system. When passenger-processing and baggage workflows lose their digital coordination layer, the resulting "reactionary delay" propagates beyond the airport perimeter into airline networks and global logistics chains. This creates a disproportionate incentive to restore service quickly, increasing susceptibility to ransom pressure even if flight safety systems remain intact.

8 Conclusion

From all verifiable information, the March 2025 KLIA cyberattack can be characterised as a significant ransomware-style incident that exploited the convergence of IT and OT systems in a highly connected airport environment [25, 2, 27]. In relation to the research questions defined in the introduction, the case shows that:

1. Complex embedded systems in airports (notably CUPPS and BHS) are highly exposed to lateral movement from compromised vendor networks when remote access, identity management, and segmentation are not tightly controlled [2, 3, **?**].

2. Manual fallbacks, while effective for preserving flight safety, are insufficient for maintaining operational efficiency at high passenger volumes and can rapidly translate technical outages into substantial delay-related financial losses [25, 29].

3. MAHB's cooperation with NACSA appears consistent with Malaysia's critical-infrastructure incident-reporting obligations under the Cyber Security Act 2024, but limited public transparency on root cause and supply-chain factors prevents a full external assessment of third-party and OT-specific risks [28, 5, 31].

More broadly, the KLIA incident illustrates how airport operators must treat vendor-managed platforms, remote support channels, and shared identity infrastructure as core elements of their threat surface rather than peripheral services, and how regulatory frameworks need to translate into enforceable, OT-aware assurance for embedded systems in critical infrastructure [33, 36, 37].

Viewed alongside other recent airport ransomware incidents, KLIA reflects a broader shift in attacker focus toward vendor-dependent, highly synchronised aviation infrastructures rather than isolated safety-critical systems.

9 Recommendation

Based on the STRIDE analysis and the regulatory and architectural gaps identified, the following real-world measures are recommended for KLIA and comparable airports:

- **Strengthen Vendor Governance:** Enforce strict Privileged Access Management (PAM), Multi-Factor Authentication (MFA), and just-in-time access for all third-party support channels entering AODB, CUPPS, or OT networks, backed by contractual requirements and regular audits of vendor security controls [36, 37].

- **Implement Immutable Backups:** To mitigate *Tampering* and ransomware impact, deploy segmented, immutable backup solutions for critical configurations and operational databases, and routinely exercise restoration procedures so that recovery is feasible without paying ransoms [29, 34].

- **Centralise Logging and Monitoring:** Address *Repudiation* risks by unifying logs from operator and vendor domains into a tamper-evident SIEM and SOC, with clear ownership of incident detection, correlation, and escalation across IT and OT [35, 18].

- **Enhance IT/OT Segmentation:** Strictly enforce and regularly validate the trust boundary between Enterprise IT and the BHS/OT network, including network zoning, unidirectional gateways where feasible, and hardened jump hosts, to limit *Elevation of Privilege* and lateral movement from vendor entry points [37, 34].

- **Operational Continuity Drills:** Regularly simulate high-volume disruption scenarios that assume partial loss of passenger-processing capabilities, in order to refine manual fallback procedures, staffing plans, and communication playbooks, thereby reducing the *Denial of Service* impact on passenger flows and airline operations [34, 29].

References

[1] Thales Group, “Aviation sector sees 600% year-on-year increase in cyberattacks,” 2025. Available: https://www.thalesgroup.com/en/news-centre/press-releases/aviation-sector-sees-600-year-year-increase-cyberattacks

[2] Condition Zebra, “The Malaysian Airport Ransomware Case: Could It Have Been Prevented?”, April 2025. Available: https://condition-zebra.com/the-malaysian-airport-ransomware-case/

[3] Sangfor, “Kuala Lumpur Airport Cyberattack: Protecting KLIA from Future Threats”, April 2025. Available: https://www.sangfor.com/blog/cybersecurity/kuala-lumpur-airport-cyberattack-protecting-klia-future-threats

[4] Passenger Terminal Today, “KLIA confirms cyber incident”, March 2025. Available: https://passengerterminaltoday.com/news/security/klia-confirms-cyber-incident.html

[5] NACSA + Malaysia Airports, “Joint Statement by National Cyber Security Agency and Malaysia Airports”, March 2025. Available: https://www.malaysiaairports.com.my/en/media-centre/news/1562

[6] Saptang Labs, “Comprehensive Cyber Threat Report”, March 2025. Available: https://saptanglabs.com/reports/threat-report-march-2025.pdf

[7] Robust IT Training, “Cyberattack on Kuala Lumpur Airport – A Wake-Up Call for Global Aviation”, March 2025. Available: https://www.robustittraining.com/blog/2025/03/28/cyberattack-on-kuala-lumpur-airport-a-wake-up-call-for-global-cybersecurity-pr

[8] International Civil Aviation Organization (ICAO), “Cybersecurity Policy Guidance,” 2025. Available: https://www.icao.int/sites/default/files/sp-files/aviationcybersecurity/Documents/Cybersecurity%20Policy%20Guidance.EN.pdf

[9] International Civil Aviation Organization (ICAO), “Aviation Cybersecurity Guidance Material,” 2025. Available: https://www.icao.int/aviation-cybersecurity/guidance-material

[10] ZeroN.One Blogs, “Kuala Lumpur Airport Cyberattack 2025: What Happened and Its Implications”, March 2025. Available: https://blogs.zeron.one/kuala-lumpur-airport-cyberattack-2025-what-happened-and-its-impact-on-aviation-

[11] Bernama, “Ransomware Strike On MAHB Highlights Need For Secure Digital Infrastructure”, March 2025. Available: https://www.bernama.com/en/news.php/?id=2406528

[12] US-ASEAN Business Council, “Cyberattack on KLIA | US-ABC Insight”, April 2025. Available: https://www.usasean.org/article/cyberattack-klia

[13] Breached.Company, “Aviation Under Siege: The 2025 Airline and Airport Cyberattack Crisis”, July 2025. Available: https://breached.company/aviation-under-siege-the-2025-airline-and-airport-cyberattack-crisis/

[14] Security Quotient, “What Malaysia’s Data Breaches Reveal: Insights for Leadership”, July 2025. Available: https://securityquotient.io/what-malaysias-data-breaches-reveal-insights-for-leadership

[15] Zavior.AI, “2025 Global Cybersecurity Breach Analysis: Comprehensive Report on Data Breaches and Cyber Attacks (January-June 2025)” January 2025. Available: https://www.zavior.ai/post/20251sthalf-breach-review

[16] Dark Reading, “Malaysian Airport’s Ransomware Attack a Warning for Asia”, April 2025. Available: https://www.darkreading.com/cyberattacks-data-breaches/malaysian-airport-cyber-disruption-warning-asia

[17] The Record, “Malaysia PM Says Country Rejected $10 Million Ransom Demand After KLIA Attack”, March 2025. Available: https://therecord.media/malaysia-pm-says-country-rejected-ransom-demand-airport-cyberattack

[18] CMS, “Threat Modeling Handbook,” August 2025. Available: https://security.cms.gov/learn/cms-threat-modeling-handbook

[19] OWASP, “Threat Modeling Process,” Available: https://owasp.org/www-community/Threat_Modeling_Process

[20] Microsoft, “Uncover Security Design Flaws Using The STRIDE Approach,” October 2019. Available: https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach

[21] KELA Cyber, “Ransomware Threat Actor Profile: Qilin,” October 2025. Available: https://www.kelacyber.com/blog/ransomware-threat-actor-profile-qilin/

[22] Check Point Research, “Qilin Ransomware (Agenda): A Deep Dive,” August 2025. Available: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/qilin-ransomware/

[23] Cybelangel, “Qilin Ransomware: Tactics & Attack Methods,” July 2025. Available: https://cybelangel.com/blog/qilin-ransomware-tactics-attack/

[24] HHS, “Qilin Threat Profile,” Available: https://www.hhs.gov/sites/default/files/qilin-threat-profile-tlpclear.pdf

[25] ICS Strive, “Ransomware Attack Disrupts Kuala Lumpur Airport,” May 2025. Available: https://icsstrive.com/incident/ransomware-attack-disrupts-kuala-lumpur-airport/

[26] Cybersecurity News, “Kuala Lumpur Airport Suffered Cyber-attack,” 2025. Available: https://cybersecuritynews.com/kuala-lumpur-airport-suffered-cyberattack/

[27] Group-IB, “Intelligence Insights APAC – March 2025,” 2025. Available: https://www.group-ib.com/resources/research-hub/intelligence-insights-apac-march-2025/

[28] Malaysia Airports Holdings Berhad (MAHB), “Media Statement on System Disruption,” 2025. Available: https://www.malaysiaairports.com.my/en/media-centre/news/1562

[29] EUROCONTROL, “Standard Inputs for Economic Analyses, Edition 10,” 2024. Available: https://www.eurocontrol.int/sites/default/files/2024-05/eurocontrol-standard-inputs-economic-analyses-ed-10.pdf

[30] Government of Malaysia, “Personal Data Protection Act 2010 (Act 709),” 2010. Available: https://mohre.um.edu.my/img/files/Personal%20Data%20Protection%20%28PDPA%29%20Act%202010.pdf

[31] Government of Malaysia, “Cyber Security Act 2024 (Act 854), Part III, Sections 17–21,” 2024. Available: https://www.zulrafique.com.my/ckfinder/userfiles/files/legislation%20update/Act854-CyberSecurityAct2024.pdf

[32] Government of Malaysia, “Cyber Security Act 2024 (Act 854),” 2024. Available: https://www.zulrafique.com.my/ckfinder/userfiles/files/legislation%20update/Act854-CyberSecurityAct2024.pdf

[33] ICAO, “Cybersecurity Policy Guidance,” 2025. Available: https://www.icao.int/sites/default/files/sp-files/aviationcybersecurity/Documents/Cybersecurity%20Policy%20Guidance.EN.pdf

[34] ICAO, “Aviation Cybersecurity Guidance Material,” 2025. Available: https://www.icao.int/aviation-cybersecurity/guidance-material

[35] ENISA, “NIS2 Technical Implementation Guidance,” 2023. Available: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

[36] ENISA, “Threat Landscape for Supply Chain Attacks,” 2021. Available: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%20for%20Supply%20Chain%20Attacks.pdf

[37] ISA / IEC, “ISA/IEC 62443 Series of Standards,” 2025. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards