I.J. Wireless and Microwave Technologies, **2025, 6, 41-53**
Published Online on December 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2025.06.04

Cybersecurity in Philippine Aviation: A Multi-Method Evaluation of Vulnerabilities and Mitigation Strategies Through Document Analysis, Case Study, and Risk Modeling

Arthur Dela Peña
Aircraft Maintenance Technology, Philippine State College of Aeronautics, 2006, Pampanga, Philippines
E-mail: artair248@gmail.com
ORCID iD: https://orcid.org/0000-0003-2519-2128
*Corresponding Author

Received: 22 November, 2024; Revised: 23 April, 2025; Accepted: 15 June, 2025; Published: 08 December, 2025

Abstract: The digitalization of aviation has heightened exposure to cyber risk, yet Philippine aviation governance and practice remain fragmented. This study evaluates sectoral vulnerabilities and feasible mitigations using a multi-method design: (i) document analysis of CAAP circulars, DICT's National Cybersecurity Plan 2022, and international guidance (ICAO, IATA, NIST, ISO/IEC 27001); (ii) case studies (Cathay Pacific breach; London Heathrow USB mishandling) chosen for analytic transferability to Philippine operations; and (iii) risk modeling via a likelihood–impact matrix with a transparent 1–5 rubric adapted from ICAO SMM, NIST SP 800-30, and DICT, scored independently by two researchers with consensus reconciliation. I integrate results through a SWOT–TOWS synthesis and propose an AI/ML feasibility roadmap tailored to on-prem/air-gapped constraints. Findings reveal high-priority risks, including unauthorized ATC access, reservation-system data breaches, and airport-network ransomware (risk score = 20), driven by monitoring gaps, legacy systems, and uneven policy enforcement. Moderately ranked threats (weak framework implementation; phishing) and under-analyzed insider risk reflect systemic and human-factor weaknesses, compounded by underreporting and limited inter-agency coordination. The study's novel contribution is a localization map that operationalizes global frameworks for Philippine conditions: phased NIST CSF adoption, tiered ISO/IEC 27001 pathways, and ICAO-aligned CAAP–DICT coordination with centralized incident reporting; plus a staged, low-cost AI/ML roadmap with KPI tracking (MTTD/MTTR, precision/recall). Limitations include the absence of primary stakeholder data and local incident/cost series; we outline a quantitative extension using operator surveys and Expected Annual Loss modeling to strengthen future empirical grounding. The results inform regulators, airlines, and airports on risk-based prioritization and practical governance upgrades to enhance national aviation cyber resilience.

Index Terms: Aviation Cybersecurity, Philippines, Risk Assessment, Policy Analysis, NIST Framework

1. Introduction

The aviation industry has become a prime target for cyberattacks due to its increasing reliance on interconnected digital systems that support critical functions, including navigation, communication, data management, and flight operations. Globally, aviation-related cyber threats have increased in frequency and complexity, posing significant risks to passenger privacy, flight safety, and national security [1,2]. Notable incidents, including ransomware attacks on airport systems and data breaches in airline networks, underscore the urgency of implementing resilient cybersecurity practices across the aviation sector. In response to these emerging challenges, international bodies such as the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), the International Civil Aviation Organization (ICAO), and the American Institute of Aeronautics and Astronautics (AIAA) have developed structured models including the NIST Cybersecurity Framework, ISO/IEC 27001, and the AIAA Aviation Cybersecurity Framework [3,4]. These frameworks aim to enhance systemic resilience, provide risk assessment protocols, and guide global aviation operators in developing security best practices.

Despite the availability of these global frameworks, implementation challenges are common in developing countries. Barriers such as limited cybersecurity awareness, talent shortages, outdated IT infrastructure, and

inconsistently enforced protocols continue to hinder the effectiveness of cybersecurity [5,6]. In the Philippine context, while aviation modernization efforts have progressed, cybersecurity governance remains underdeveloped. Agencies such as the Civil Aviation Authority of the Philippines (CAAP) and the Department of Information and Communications Technology (DICT) have introduced national digital security strategies, but these policies lack aviation-specific provisions. For instance, the National Cybersecurity Plan 2022 provides overarching guidance on critical infrastructure protection but does not explicitly address aviation operations and their unique cyber vulnerabilities [7]. This lack of sector-specific integration leaves Philippine aviation increasingly exposed to evolving cyber threats.

The foundation of this study rests on the Confidentiality, Integrity, and Availability (CIA) triad, which serves as the core principle of information security [8]. Complementing this theoretical base are applied risk assessment models, such as NIST SP 800-30 and ISO/IEC 27005, as well as structured decision frameworks, including Monte Carlo simulations and SWOT-style prioritization [9,10]. These models not only offer tools for qualitative risk assessment but also shape the analytical framework for this study. Specifically, the selection of case studies focusing on real-world incidents involving major airlines and airports—and the design of the contextual risk matrix were guided by the logic and methodology of these internationally recognized frameworks. In this way, global best practices not only inform the background of this study but also underpin its entire research structure, guiding the evaluation of threats, vulnerabilities, and mitigation strategies within the Philippine aviation context.

To date, no comprehensive study in the Philippine context has integrated document analysis, case-based incident review, and contextual risk modeling to evaluate aviation cybersecurity. This research addresses that gap by applying an interdisciplinary framework that bridges theoretical models with localized risk data.

Given these considerations, the study adopts a multi-method approach to evaluate cybersecurity vulnerabilities and mitigation strategies in Philippine aviation. The methodology integrates document analysis of existing regulations and international frameworks, case study evaluations of real-world cyber incidents, and a risk modeling process using a likelihood-impact matrix informed by global standards. This design enables a more nuanced, evidence-based understanding of the current cybersecurity posture within the local aviation landscape, providing context-specific recommendations that can inform both policy and practice.

This research is significant to various stakeholders in the aviation industry. For regulatory agencies like CAAP and national bodies such as DICT, the findings provide actionable insights for crafting aviation-specific cybersecurity policies and harmonizing efforts across sectors. Airlines and airport operators may leverage the study's outcomes to prioritize risk areas, enhance cyber training, and adopt international standards. Likewise, cybersecurity professionals and academic researchers will benefit from the study's integrated model, which can be adapted for broader assessments of critical infrastructure. Ultimately, this study fills a crucial gap in aviation cybersecurity research in the Philippine context by offering a replicable, interdisciplinary framework that bridges global theory with local practice.

2. Review of Related Literature

2.1 Cybersecurity Frameworks in Aviation

The aviation industry faces increasing cybersecurity challenges as it becomes more digitally integrated. Several frameworks have been proposed to address these challenges, including the AIAA Aviation Cybersecurity Framework [3] and a graph-based communication-oriented framework [11]. These frameworks emphasize the importance of risk assessment and management [3]. A socio-technical systems approach is recommended to address both technical and human factors in cybersecurity [12, 13, 14]. This approach recognizes the complex interplay of social, technical, and environmental factors in aviation cybersecurity. Trustworthiness requirements and models are crucial for aviation systems [15], as is seamless interoperability underpinned by cybersecurity [16]. These frameworks and approaches aim to enhance the resilience and security of aviation systems in an increasingly interconnected and technologically advanced environment.

2.2 Global Overview of Cybersecurity in Aviation

Cybersecurity in aviation is a growing concern as the industry increasingly relies on digital technologies. Key challenges include protecting air traffic control systems, aircraft communications, and navigation systems from cyber threats [8,17]. The transition to NextGen and satellite-based systems has introduced new vulnerabilities [7,9]. High-profile incidents have underscored the need for enhanced cybersecurity measures, with threats ranging from data breaches to the potential hijacking of aircraft systems [20,21]. Artificial intelligence and machine learning are being explored as possible solutions for enhancing aviation cybersecurity [15]. The rise of unmanned aircraft systems (UAS) presents additional cybersecurity challenges [22]. To address these issues, experts recommend developing comprehensive cybersecurity frameworks, conducting thorough risk assessments, and implementing robust security measures across all aviation systems [5, 19].

2.3 Cybersecurity in Philippine Aviation

Cybersecurity in aviation is a growing concern as increasing technological integration expands the attack surface. Key challenges include limited resources, insider threats, and the security of operational technologies [5]. Emerging tools such as Artificial Intelligence (AI) and Machine Learning (ML) offer promise for anomaly detection and securing data link communications [15]. Threats range from malware to potential aircraft system takeovers [23], underscoring the need for proactive measures such as policy reforms and structured cyber risk management systems [24]. Advanced Persistent Threat (APT) groups further exacerbate risks to aviation IT infrastructure [20], reinforcing calls for a coordinated, multi-stakeholder approach to governance [1,25].

In the Philippine context, reliance on digital infrastructure exposes persistent vulnerabilities. The January 2023 outage at the NAIA Air Traffic Management Center disrupted over 56,000 passengers, revealing gaps in redundancy and resilience, even though the event was not classified as a cyberattack. Likewise, agencies such as the DICT and the Philippine Army have reported intrusion attempts, confirming the presence of advanced cyber threats across critical sectors. While publicly documented aviation-specific cyber incidents remain limited, these cases illustrate the fragility of national systems and highlight the urgency of aviation-focused cybersecurity strategies. International frameworks such as ISO/IEC 27001, NIST CSF, and ICAO guidance provide global benchmarks; their adaptation to the Philippine setting is examined in Section 4.1.1 and summarized in Table 3.

2.4 Vulnerabilities in Aviation Systems

Aviation systems are vulnerable to numerous cybersecurity threats, encompassing both technical and human factors. Critical infrastructure, like Instrument Landing Systems (ILS) and VHF Omnidirectional Range (VOR), is susceptible to attacks [26]. Aircraft systems, particularly those exposed via communication and satellite systems, are vulnerable to cyber threats [27]. The integration of Information and Communication Technology (ICT) in aviation has increased attack surfaces, with Advanced Persistent Threat (APT) groups posing significant risks [20]. Mobile cockpit information systems used by pilots are also vulnerable to manipulation [28]. The Automated Dependent Surveillance-Broadcast (ADS-B) system, while promising for air traffic management, has inherent security weaknesses due to its reliance on wireless networks [29]. To address these challenges, comprehensive threat models, risk assessments, and mitigation strategies are necessary [30].

2.5 Mitigation Strategies in Aviation Cybersecurity (revised)

The digitization of aviation systems introduces vulnerabilities in communication, navigation, and surveillance networks, with ADS-B being among the most exposed [18, 21, 29]. Core mitigation measures include encryption, firewalls, and intrusion detection systems, complemented by workforce training and awareness campaigns to address human factors [5,19]. The COVID-19 period highlighted the urgency of such measures, with phishing and ransomware attacks becoming more prevalent [19].

Emerging solutions such as AI and machine learning can support anomaly detection, phishing defense, and data-link security [31]. In the Philippine context, their adoption is feasible in staged, low-cost applications (e.g., log anomaly detection, phishing analytics, and endpoint triage) using existing SIEM and EDR infrastructure. At the same time, more advanced deployments require improved data readiness and skilled personnel. Looking ahead, cybersecurity must be embedded early in system design, particularly for electric aircraft charging infrastructure, to prevent the creation of new digital attack surfaces [32].

2.6 Research Gaps

Current literature reveals several critical research gaps in Philippine aviation cybersecurity. There is a lack of localized studies that address sector-specific challenges such as resource constraints, fragmented regulations, and infrastructure limitations. Although international standards, such as ISO 27001 and NIST, are referenced, their enforcement and effectiveness in the local context remain unclear. The adoption of emerging technologies, such as AI and machine learning, is underexplored, and insider threats, despite being high-risk, have not been sufficiently assessed in Philippine operations. Advanced Persistent Threats (APTs) also lack localized analysis, leaving resilience levels uncertain. Furthermore, comprehensive risk assessments tailored to aviation systems, such as air traffic control and communication networks, are scarce. New technologies such as unmanned aircraft systems and electrification raise cybersecurity concerns that remain unaddressed. The sector's pandemic-related cyber risks, training program effectiveness, and engagement in global cybersecurity efforts are poorly documented. Finally, socio-technical perspectives and localized threat models tailored to Philippine aviation are mainly absent from current research.

3. Methodology

3.1 Research Design

This study adopted a qualitative-descriptive research design utilizing a multi-method approach that integrated document analysis, case study investigation, and risk modeling. The qualitative-descriptive design was appropriate for

exploring and interpreting complex, context-specific phenomena, such as cybersecurity in aviation, through non-numerical data. By combining multiple methods, the study aimed to develop a comprehensive understanding of cybersecurity vulnerabilities and mitigation strategies within the Philippine aviation sector. This design enabled a layered exploration of the subject by drawing insights from policy documents, real-world cases, and structured risk assessment frameworks, allowing for a holistic evaluation of the cybersecurity landscape in aviation.

3.2 Data Sources

This study draws on three source groups: documents, case studies, and risk-modeling tools. Documents include CAAP circulars and advisories, DICT's *National Cybersecurity Plan 2022*, ICAO and IATA guidance, and control standards (NIST SP 800-30; ISO/IEC 27001), as well as airline cybersecurity policies where accessible. Case studies were purposefully selected for analytic transferability: the Cathay Pacific data breach and the London Heathrow USB mishandling incident represent two dominant risk archetypes—enterprise data compromise and physical data loss. These incidents are extensively documented (including regulator findings), enabling transparent coding of causes, controls, and responses. Given limited public disclosure of aviation-specific cyber incidents in the Philippines, these international exemplars serve as methodological anchors and are triangulated with localized evidence (e.g., NAIA ATMC outage; government intrusion reports) to ensure contextual relevance.

Risk-modeling tools include a likelihood–impact matrix and SWOT-style assessments, with threats and mitigations mapped to NIST CSF functions (Identify/Protect/Detect/Respond/Recover). While the present study is primarily qualitative, the framework is designed to be complemented by quantitative extensions—such as operator surveys and Expected Annual Loss (EAL) modeling—to incorporate incident frequencies and cost estimates in future research. This multi-source design grounds findings in policy analysis, auditable incident evidence, and structured risk evaluation tailored to the Philippine aviation sector.

3.3 Data Analysis Procedures

The data collected in this study were analyzed using a combination of qualitative techniques tailored to each data source. The analysis followed three primary approaches: thematic coding for document analysis, framework-based analysis for case studies, and qualitative risk scoring using a likelihood-impact matrix. These methods ensured a structured evaluation of cybersecurity vulnerabilities and mitigation strategies in the Philippine aviation sector.

For the document analysis, a thematic coding approach was employed to identify recurring patterns, concepts, and gaps within regulatory documents, policies, and cybersecurity frameworks. Key texts, including CAAP circulars, ICAO cybersecurity guidelines, airline cybersecurity policies, and DICT plans, were systematically reviewed and coded based on common themes such as regulatory compliance, risk management strategies, and implementation challenges. This process enabled the identification of critical areas where Philippine aviation cybersecurity policies aligned with or diverged from international standards.

For the case study analysis, a framework-based approach was employed to evaluate real-world cyber incidents and security breaches affecting the aviation sector. The selected cases, sourced from news reports, incident records, and official statements, were analyzed using structured frameworks such as the Five Ws (Who, What, When, Where, and Why) and cyber incident response models. This method provided a systematic way to assess the causes, impact, and resolution of each incident, while highlighting key vulnerabilities in the aviation sector.

Lastly, a qualitative risk scoring method was applied using a likelihood-impact matrix to assess identified cybersecurity risks. Threats were categorized based on their probability of occurrence and potential impact on aviation operations. This matrix enabled the prioritization of cybersecurity risks, providing a structured basis for recommending effective mitigation strategies. Additionally, the results from the thematic and case study analyses informed the qualitative risk assessment, ensuring that the scoring was grounded in both policy evaluation and real-world incident data.

By integrating these analytical techniques, the study employed a multi-layered approach to understanding aviation cybersecurity risks, enabling data-driven conclusions and actionable recommendations.

3.4 Ethical Considerations

This study adhered to ethical research standards by ensuring that all data sources were obtained from publicly available materials, eliminating the need for human respondents or direct participant involvement. The research relied solely on published documents, regulatory frameworks, case study reports, and risk assessment models, ensuring compliance with ethical guidelines for data collection. Proper citation and attribution were strictly followed to acknowledge original authorship and intellectual property rights, maintaining academic integrity and preventing any form of plagiarism. Additionally, all analyzed materials were used within the scope of fair use, with no modifications that could misrepresent the original context or intent of the sources.

4. Results and Discussion

4.1 Document Analysis

[Table 1] shows that cybersecurity in Philippine aviation remains fragmented and underdeveloped. CAAP circulars continue to emphasize physical safety and airworthiness, but give limited attention to digital threats such as data breaches and infrastructure vulnerabilities. The DICT's *National Cybersecurity Plan 2022* outlines broad national priorities but does not provide aviation-specific provisions, creating a gap between national policy and sectoral needs. Weak inter-agency coordination among CAAP, DICT, and aviation operators further contributes to fragmented enforcement and uneven preparedness.

Across airlines and airports, cybersecurity maturity is inconsistent. Some operators have adopted baseline measures, such as firewalls and awareness training; however, the absence of a unified aviation cybersecurity framework and underreporting of incidents obscure the actual risk environment. This reinforces the need for standardized reporting protocols, coordinated oversight, and scalable governance mechanisms.

Global models—ICAO's Aviation Cybersecurity Strategy, IATA's Cybersecurity Toolkit, NIST CSF, and ISO/IEC 27001—provide comprehensive governance structures, but their relevance depends on tailored application. For example, ICAO guidance could be operationalized through CAAP–DICT coordination to reduce regulatory silos; NIST CSF's *Identify* and *Detect* functions can be prioritized for asset inventories and monitoring in resource-limited airports; and ISO/IEC 27001 certification pathways could be phased, starting with major carriers and gradually extended to regional operators. These adaptations recognize local constraints—limited budgets, uneven technical expertise, and weak mandates—while aligning the sector with global benchmarks.

In sum, while frameworks and policy tools exist, the Philippine aviation sector still lacks an integrated, aviation-specific cybersecurity strategy. Bridging this gap requires contextualizing international standards into scalable local practices, strengthening regulatory oversight, and institutionalizing cross-sector collaboration to build resilience against evolving digital threats.

To move beyond general applicability, [Table 2] illustrates how international frameworks can be operationalized within the Philippine aviation sector. The adaptations highlight context-specific measures that account for regulatory gaps, resource constraints, and varying operator capacities.

Table 1. Synthesis of Document Analysis Findings.

Category	Key Findings	Gaps/Challenges	Implications / Needed Actions
Philippine Aviation Regulations (CAAP Circulars)	Focus on physical safety/airworthiness; limited explicit provisions for cyber risks (data breaches, digital infrastructure).	Enforcement on cybersecurity is limited; fragmented CAAP–DICT–operator coordination.	Issue aviation-specific cyber regs; mandate NIST/ISO alignment; formal CAAP–DICT MoU; centralized incident reporting.
Cybersecurity Plans in Philippine Aviation (Airlines/Airports)	Preparedness varies; basic controls and awareness training exist in some institutions.	No standardized national framework; underreporting due to a lack of a formal reporting mechanism.	Set sector baseline controls, require periodic audits, implement a national reporting portal, and establish capacity-building programs.
International Frameworks (ICAO, IATA, NIST, ISO/IEC 27001)	Comprehensive governance/risk models available; IATA guidance is non-binding; adoption limited by resources and skills.	Inconsistent local implementation; budget and talent constraints delay uptake.	Tailor frameworks to the PH context; phased adoption roadmap; targeted funding; workforce upskilling and certification.

Table 2. International Cybersecurity Frameworks and Their Local Adaptation in Philippine Aviation.

Framework	Core Functions / Controls	Local Adaptation for Philippine Aviation
ICAO Aviation Cybersecurity Strategy	Global benchmarks for governance, risk management, and information sharing	Operationalized through a CAAP–DICT coordination mechanism to reduce siloed oversight and establish a centralized incident reporting portal.
IATA Cybersecurity Toolkit	Best practices for airlines (network security, data protection, awareness programs)	Used as voluntary guidance but phased into CAAP advisories; tailored checklists developed for central vs. regional carriers to reflect resource differences.
NIST Cybersecurity Framework (CSF)	Identify, Protect, Detect, Respond, Recover functions	Prioritize Identify (asset inventories) and Detect (threat monitoring) as immediate baselines; scale advanced functions in phases according to operator capacity and funding.
ISO/IEC 27001	Formal information security management systems (ISMS)	Introduce tiered certification pathways, starting with large carriers and international airports, and then expanding to regional operators with simplified compliance templates.

4.1.1 Local Adaptation of Global Frameworks

As highlighted in Section 2.3, international frameworks such as ICAO's *Aviation Cybersecurity Strategy*, IATA's *Cybersecurity Toolkit*, the NIST Cybersecurity Framework (CSF), and ISO/IEC 27001 provide established global benchmarks. However, their direct adoption in the Philippines is constrained by limited regulatory mandates, uneven

technical expertise, and resource disparities across operators. To strengthen sectoral resilience, these frameworks must be localized into scalable and enforceable practices.

This study proposes three priority adaptations. First, ICAO guidance can be operationalized through formal CAAP–DICT coordination, reducing siloed oversight and enabling a centralized incident reporting system. Second, the NIST CSF's *Identify* and *Detect* functions should be prioritized as immediate baselines for asset inventories and monitoring in resource-constrained airports, with advanced functions phased in over time. Third, ISO/IEC 27001 adoption can follow a tiered pathway, with certification initially mandated for major carriers and international airports, and later extended to regional operators using simplified templates. Meanwhile, the IATA toolkit, though non-binding, can be integrated into CAAP advisories with checklists tailored to operator size and maturity.

These measures extend beyond general applicability, translating broad frameworks into context-specific strategies tailored to the Philippine aviation sector. [Table 3] summarizes the alignment of international standards with local needs, offering regulators and operators a practical map for phased and resource-sensitive implementation.

Table 3. Adaptation of International Cybersecurity Frameworks to Philippine Aviation.

Framework	Core Focus	Localized Application in the Philippines
ICAO Aviation Cybersecurity Strategy	Global governance, risk management, and information sharing	Operationalize via CAAP–DICT coordination and establish a centralized incident reporting system.
IATA Cybersecurity Toolkit	Airline-level best practices (network security, data protection, awareness)	Integrate into CAAP advisories; adapt checklists for large vs. regional operators.
NIST Cybersecurity Framework (CSF)	Identify, Protect, Detect, Respond, Recover	Prioritize Identify (asset inventories) and Detect (monitoring) as baselines; phase in advanced functions as capacity grows.
ISO/IEC 27001	Information Security Management Systems (ISMS)	Implement tiered certification, mandating it for major carriers and hubs first, and extend it later to smaller operators with simplified templates.

4.2 Case Study Analysis

The comparative analysis in [Table 4] examines two archetypal incidents—Cathay Pacific (2018) and London Heathrow (2017)—purposefully selected to cover enterprise data-breach and physical data-mishandling modes. These map onto the dominant risk categories in our Philippine model and are regulator-documented, enabling the reproducible coding of causes, controls, and responses. They therefore serve as methodological anchors where local aviation cyber incident data are sparse, while preserving transferability to the Philippine context.

In the Cathay Pacific breach, unauthorized access exposed 9.4 million passenger records; delayed disclosure (~7 months) and a £500,000 ICO penalty highlighted gaps in monitoring, transparency, and data protection.

In the Heathrow case, an unencrypted USB containing sensitive security data revealed weaknesses in handling and access control; despite a swift internal response, the airport received a £120,000 ICO fine and implemented training and policy reforms.

Table 4. Comparative Case Study Analysis of Two Aviation Cybersecurity Incidents.

Category	Case 1: Cathay Pacific Data Breach (2018)	Case 2: London Heathrow USB Drive Incident (2017)
Incident	A data breach exposed the personal information of 9.4 million passengers, including passport numbers and credit card details.	An unprotected USB drive containing sensitive airport security data was discovered on a public street, posing a national security risk.
Date of Occurrence	March 2018 (Detected) – October 2018 (Disclosed)	October 2017 (Discovered)
Cause of Breach	Unauthorized access to IT systems and exploitation of weak security measures.	Failure to encrypt and secure highly sensitive data can lead to data loss due to mishandling.
Response Actions	- Conducted an internal investigation with cybersecurity experts. - Implemented security enhancements. - Notified affected customers and coordinated with regulators.	- Launched an internal security review. - Revised data handling policies and improved employee training on cybersecurity. - Implemented new encryption and access control measures.
Consequences	- Regulatory Fine: £500,000 by the UK ICO for failing to protect passenger data. - Reputational Damage: Public backlash due to delayed disclosure. - Operational Impact: Increased security costs and stricter data protection measures are required.	- Regulatory Fine: £120,000 by the UK ICO for failing to protect sensitive security data. - Operational Risk: Exposure of airport security protocols, potentially compromising national security. - Policy Changes: Stricter controls on data storage, encryption, and employee cybersecurity training.
Effectiveness of Response	Weak initial response due to delayed detection and disclosure. Post-incident security improvements were made, but faster mitigation could have reduced damage.	A rapid internal response prevented the immediate exploitation of leaked data. However, poor initial data handling practices exposed significant gaps in cybersecurity awareness and compliance.
Lessons Learned	- Real-time threat monitoring and early detection are crucial. - Transparent disclosure policies are necessary to maintain public trust. - Stronger encryption and access controls are required for passenger data.	- Strict policies on handling sensitive airport security data must be enforced. - Encryption and access restrictions should be mandatory for all confidential files. Regular cybersecurity training is crucial in preventing human errors.

Together, these cases demonstrate that aviation cyber risk spans both digital systems and physical processes, motivating controls relevant to Philippine operators, including real-time detection, encryption, and access governance, as well as proactive incident response and continuous workforce training—aligned with ICAO/NIST/ISO guidance and our risk-prioritization results. I triangulate these patterns with localized evidence (e.g., the 2023 NAIA ATMC outage and reported government intrusion attempts) to define sector-specific boundary conditions for the Philippines.

4.3 Risk Assessment Modeling

[Figure 1] presents the prioritization of cybersecurity risks in Philippine aviation using a likelihood–impact matrix. Each threat was assessed on three dimensions—likelihood of occurrence, impact severity, and vulnerability level—with the overall risk score defined as:

$$R = L \; x \; I \tag{1}$$

where R is the risk score, L is likelihood, and I is impact. To enhance transparency, scores on a 1–5 scale were assigned using a structured rubric adapted from ICAO's *Safety Management Manual*, NIST SP 800-30, and the DICT's *National Cybersecurity Plan 2022*. Likelihood reflected the observed frequency of similar incidents globally and in Philippine advisories; impact ranged from minor disruption (1) to national-level operational or safety failure (5); and vulnerability captured the extent to which technical and organizational controls were absent, partial, or present. Two researchers independently applied the rubric, with discrepancies reconciled through consensus to minimize subjectivity.

The results show that the highest-priority threats (risk score = 20) are unauthorized access to air traffic control systems, data breaches in airline reservation systems, and ransomware attacks on airport networks. These scored the maximum on both likelihood and impact (5×4 or 4×5) and exhibited high vulnerability (5), underscoring urgent gaps in aviation cyber defenses. Moderately high risks include weak implementation of international frameworks (score 16) and phishing attacks on personnel (score 15), reflecting systemic and human-factor vulnerabilities. Lower-ranked threats, such as loss of sensitive data via portable devices (score 12) and insider threats (score 9), remain relevant as they expose persistent weaknesses in data handling, access control, and staff training.

Although insider threats received a lower score, they warrant closer attention in the Philippine context. Shared account practices, limited enforcement of least-privilege policies, and reliance on contractual IT staff increase the risk of undetected misuse. Cultural factors, such as hierarchical workplace norms and *pakikisama* (the avoidance of conflict to preserve harmony), may also discourage employees from reporting suspicious behavior. While publicly documented aviation-specific insider cases are scarce, parallels from DICT advisories and other government systems confirm that insider misuse is a tangible risk. Addressing this requires stricter vetting and exit protocols, continuous monitoring of privileged accounts, and fostering a culture of reporting that reduces stigma and protects whistleblowers.

Overall, the likelihood–impact matrix demonstrates that Philippine aviation faces an interplay of technological, procedural, and human-centric risks. The findings underscore the urgent need for proactive measures, including real-time threat monitoring, encryption of sensitive data, and standardized incident reporting, along with the phased implementation of international frameworks as outlined in Section 4.1.1 and [Table 3], to enhance national aviation cyber resilience.

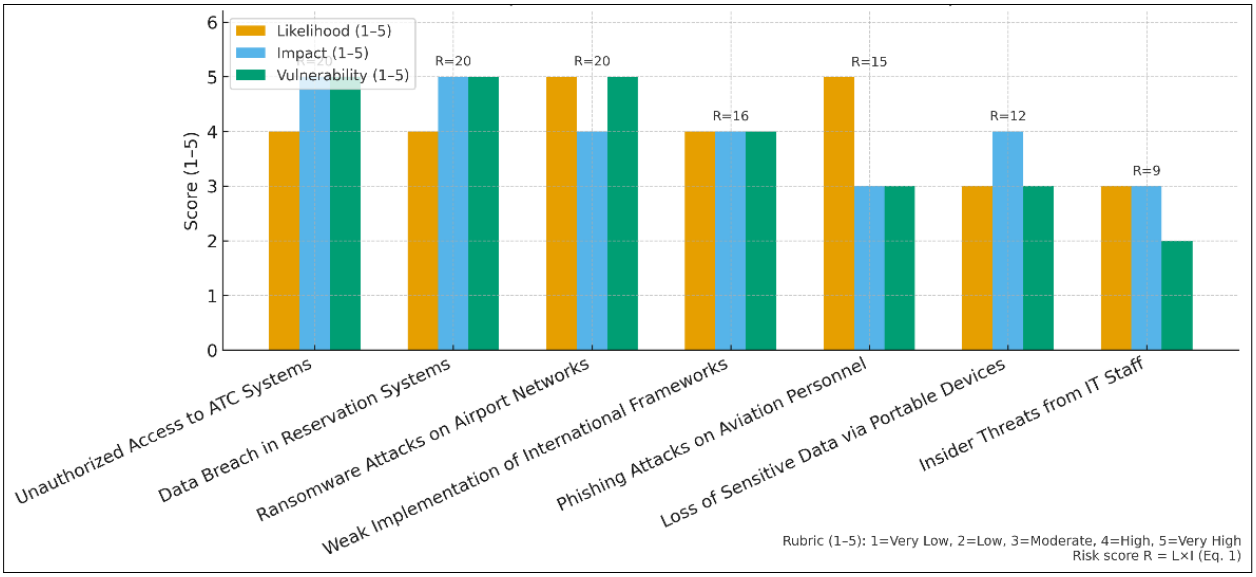

Fig. 1. Likelihood, Impact, and Vulnerability (1–5) by threat category; annotations show Risk score R=L×IR=L\times IR=L×I per Eq. (1).

[Figure 2] visualizes the distribution of risk scores for the most pressing cybersecurity threats in Philippine aviation, while [Table 5] quantifies these findings by detailing the likelihood, impact, vulnerability, and overall risk scores for each threat. The three highest-priority risks—unauthorized access to air traffic control systems, data breaches in airline reservation systems, and ransomware attacks on airport networks—each scored 20, reflecting both high likelihood of occurrence and catastrophic potential for operational continuity, passenger safety, and national security. Slightly lower but still significant are the weak implementation of international frameworks (score of 16) and phishing attacks on aviation personnel (score of 15), which stem from systemic and human-factor weaknesses such as inconsistent policy adoption, limited regulatory enforcement, and inadequate cybersecurity awareness.

At the lower end of the spectrum, loss of sensitive data via portable devices (score of 12) and insider threats from IT staff (score of 9) appear less critical but remain persistent risks in environments with weak data protection protocols and access controls. Together, the chart and table emphasize the importance of risk-based prioritization in shaping cybersecurity strategy and resource allocation. Addressing the highest-ranking threats with urgency, while simultaneously reinforcing foundational policies and workforce training, will be essential to strengthening the resilience of Philippine aviation against evolving cyber threats.

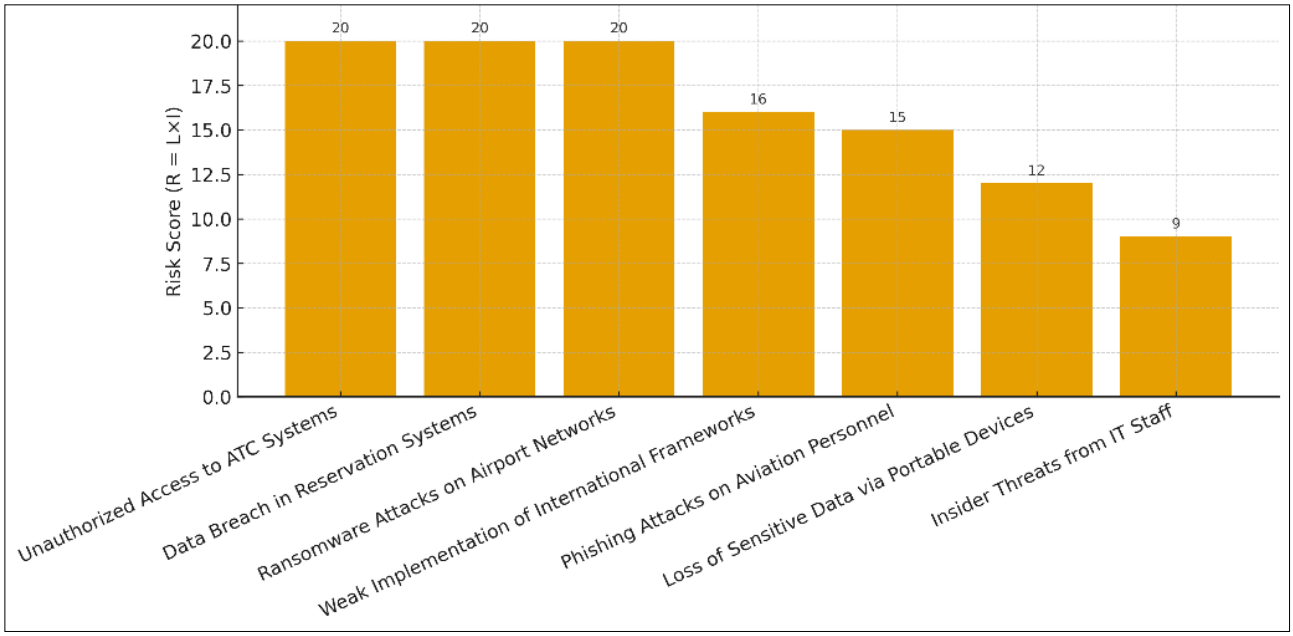

Fig. 2. Risk score R=L×IR=L\times IR=L×I by threat category (descending); higher bars indicate higher urgency.

Table 5. Likelihood, Impact, Vulnerability, and Risk Scores for Seven Cybersecurity Threats in Philippine Aviation.

Threat Category	Likelihood (L)	Impact (I)	Vulnerability (V)	Risk Score (R = L ×I)
Unauthorized Access to ATC Systems	4	5	5	20
Data Breach in Reservation Systems	4	5	5	20
Ransomware Attacks on Airport Networks	5	4	5	20
Weak Implementation of International Frameworks	4	4	4	16
Phishing Attacks on Aviation Personnel	5	3	3	15
Loss of Sensitive Data via Portable Devices	3	4	3	12
Insider Threats from IT Staff	3	3	2	9

4.3.1 SWOT Results and Strategic Prioritization

I synthesized findings from document analysis (S 4.1), case studies (S 4.2), and the risk matrix (S 4.3) into a concise SWOT (Table 6). Strengths include partial alignment with ICAO/NIST/ISO and ISO, as well as growing awareness; weaknesses include limited aviation-specific regulation, underreporting, and resilience gaps. Opportunities lie in a phased, sector-tailored rollout of NIST/ISO controls and CAAP–DICT coordination; threats center on high-impact risks (ATC access, data breaches, and ransomware) and human-factor vectors (phishing and insider risks).

To translate SWOT into action, Table 6 applies a TOWS lens, linking strengths/opportunities to near-term wins (e.g., baseline controls, targeted training) and addressing weaknesses/threats via governance (CAAP–DICT MoU, incident portal) and resilience (redundancy, immutable backups). These strategies align with NIST CSF functions and with the risk priorities in Table 3, specifying owners and horizons.

Table 6. Integrated SWOT–TOWS Summary for Philippine Aviation Cybersecurity.

Type	Key Finding / Strategy	Implication / Action (NIST)	Reference
S	Partial alignment with ICAO/NIST/ISO in some operators; awareness programs exist.	Phase in baseline controls (Levels 1–3) across operators; map to ID, PR, DE, RS	S4.1; Table 1
S	National baseline via DICT's NCSP 2022	Use as a policy anchor to formalize aviation-specific controls and audits	S4.1; Table 1
W	Limited aviation-specific cyber regulation/enforcement	Issue CAAP aviation-cyber circular; institute sector audits; align to ID.GV/PR	S4.1; Table 1
W	Underreporting; no formal incident portal	Create a centralized portal with disclosure SLAs; improve ID.AM/DE.DP	S4.1; S4.X SWOT
W	Resilience gaps in critical digital infrastructure	Mandate redundancy/failover drills; immutable/offline backups	S4.2 (NAIA ATMC 2023)
O	Sector-tailored rollout of NIST/ISO/ICAO	Publish phased roadmap; certify maturity per NIST functions	Table 3
O	Formalize CAAP–DICT coordination	MoU for governance, incident sharing, and joint audits	Table 3
O	Targeted capacity building (SOC, forensics, phishing sims)	Fund training and exercises; measure PR.AT/DE.AE improvements	Table 3
T	High-impact risks: ATC access, data breach, ransomware	Zero-trust/PAM/MFA; EDR/SIEM; segmentation; backups & IR playbooks	Fig. 2; Table 3
T	Human factors: phishing, insider risks	Role-based training; simulated phishing; email auth (SPF/DKIM/DMARC)	S4.3; Table 3
T	Supply-chain/device risks (portable media, contractors)	Device encryption/MDM; removable-media controls and logging	S4.2; S4.3

4.3.2 AI/ML Feasibility and Phased Roadmap (Philippine Setting)

The feasibility of AI and machine learning applications in Philippine aviation cybersecurity was evaluated across three dimensions: data readiness, compute footprint, and operational fit for air-gapped or intermittently connected environments. To balance potential impact with resource constraints, a phased roadmap is proposed. In Phase 1 (0–3 months), the focus is on establishing baselines through log normalization, a minimum 90-day log retention policy, and the deployment of simple anomaly rules. This stage also introduces model governance mechanisms, including versioning and monthly drift checks. Phase 2 (3–6 months) advances to unsupervised pilots by deploying on-premise log and network anomaly models, together with User and Entity Behavior Analytics (UEBA) baselines. Thresholds are calibrated through human-in-the-loop review, with performance monitored using mean time to detect (MTTD) and precision/recall metrics. Phase 3 (6–12 months) introduces supervised add-ons, including phishing classifiers, training analytics, and endpoint detection and response (EDR) triage models. This stage also establishes automated playbooks for escalation and rollback, with performance tracked through mean time to respond (MTTR) and incident closure rates.

Risk and ethics safeguards are integrated throughout the roadmap. Models are designed to operate with the least privilege, avoiding the use of personally identifiable information (PII) beyond operational necessity. A fallback to manual triage is maintained to ensure operational continuity. Quarterly performance reviews evaluate precision, recall, MTTD, and MTTR, while red-team testing identifies overfitting and potential bias. Each use case directly addresses threats prioritized in [Table 3]. For example, ransomware is mitigated through EDR triage and immutable backups, phishing is addressed through classifiers and training analytics, and insider risks are managed through UEBA baselining.

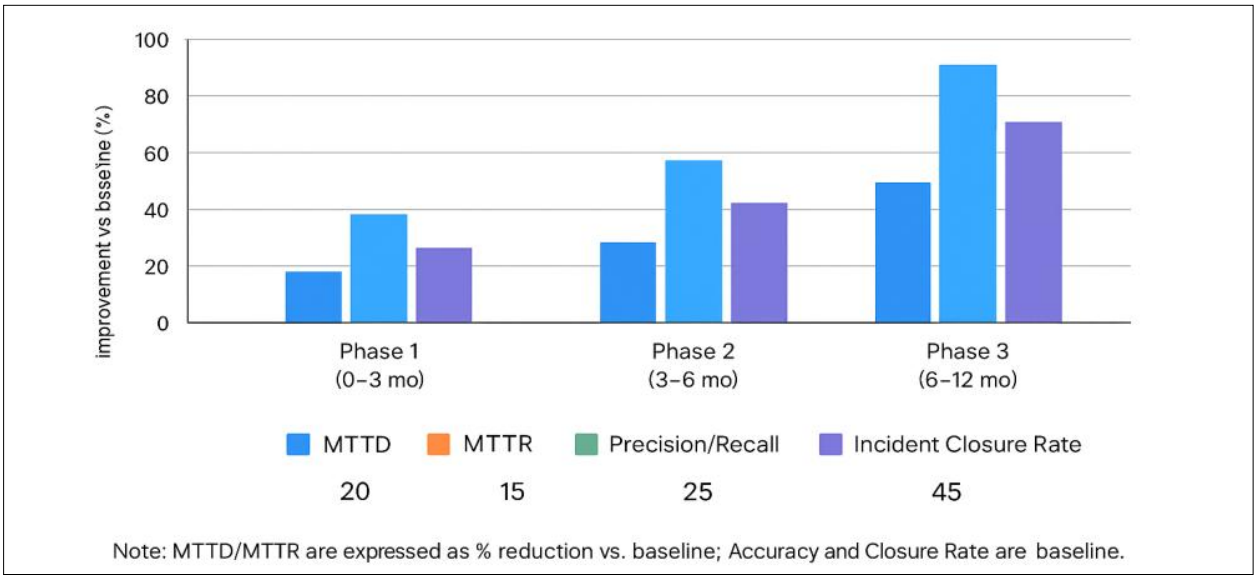

Fig. 3. KPI Improvements across Phased AI/ML Adoption in Philippine Aviation Cybersecurity.

4.4 Cybersecurity Risk-Response Alignment Matrix

[Table 7] presents a strategic overview of the critical cybersecurity threats facing Philippine aviation, mapped against institutional response readiness and the severity of the gaps. The top three risks—unauthorized access to air traffic control systems, ransomware attacks on airport networks, and data breaches in reservation systems all have the highest risk score of 20. However, two of them (ATC access and reservation systems) exhibit low readiness and high severity gaps, indicating urgent vulnerabilities that require immediate attention. Recommended actions include upgrading access control mechanisms, enforcing encryption, and enhancing cybersecurity awareness and training.

The weak implementation of international frameworks (risk score: 16) and phishing attacks on aviation personnel (score: 15) reveal systemic and human-centric issues, where the response remains low to moderate. These highlight the need for more vigorous regulatory enforcement and consistent training programs across the sector. Meanwhile, lower-scoring threats, such as the loss of sensitive data via portable devices and insider threats from IT staff, still require targeted mitigation, mainly through encryption mandates and insider risk controls.

Overall, the matrix reinforces the study's findings that while critical risks are known, response readiness remains inconsistent, particularly in high-impact domains. Strengthening cybersecurity in Philippine aviation will require not only technical upgrades but also policy standardization, cross-agency coordination, and a national cybersecurity enforcement framework tailored for aviation environments.

Table 7. Core Risk–Response Matrix for Philippine Aviation.

Threat Category	Risk Score	Current Readiness	Gap Severity	Priority
Unauthorized Access to ATC Systems	20	Low	High	Critical
Ransomware Attacks on Airport Networks	20	Medium	Medium	High
Data Breach in Reservation Systems	20	Low	High	High
Weak Implementation of International Frameworks	16	Low	High	High
Phishing Attacks on Aviation Personnel	15	Medium	Medium	Medium-High
Loss of Sensitive Data via Portable Devices	12	Medium	Medium	Medium
Insider Threats from IT Staff	9	Low	Medium	Medium

4.5 Cyber Security Risks and Response Readiness

[Figure 3] provides a heat map visualization of cybersecurity risks in Philippine aviation, comparing three key dimensions: Risk Score, Response Readiness, and Gap Severity across seven major threat categories. The darkest red areas correspond to the most critical concerns, which are characterized by high risk scores, low response readiness, and severe gap severity.

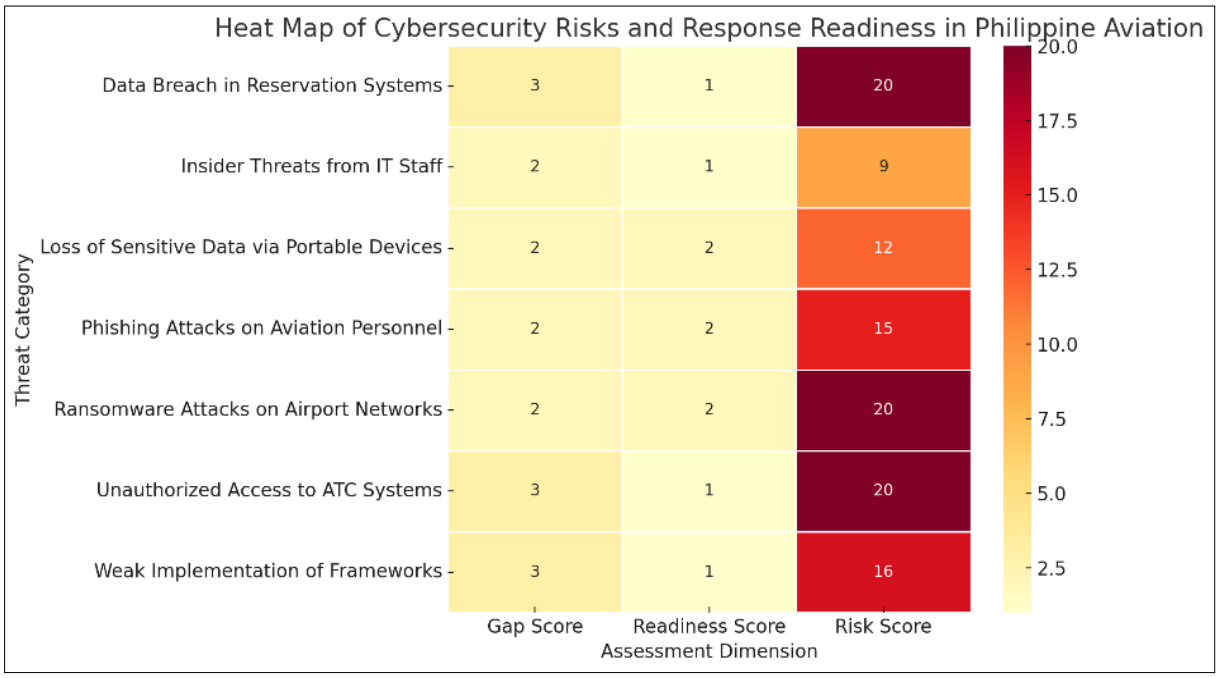

Fig. 4. Heat Map of Cybersecurity Risks and Response Readiness in Philippine Aviation

The threats with the most alarming profiles are Unauthorized Access to Air Traffic Control (ATC) Systems, Data Breaches in Reservation Systems, and Ransomware Attacks on Airport Networks. These threats show high risk scores and low to medium response readiness, with critical gaps that emphasize the need for immediate and comprehensive mitigation. This aligns with earlier findings that these categories present the greatest danger to aviation safety and operational continuity, yet remain underprotected due to outdated systems and insufficient monitoring protocols.

Meanwhile, Weak Implementation of International Frameworks and Phishing Attacks on Aviation Personnel also score significantly, but with slightly higher readiness levels. These threats reflect ongoing issues in regulatory compliance and cybersecurity awareness, highlighting systemic and human-factor vulnerabilities that necessitate policy enforcement and capacity-building strategies to address.

In contrast, Loss of Sensitive Data via Portable Devices and Insider Threats from IT Staff show lower risk scores, but still exhibit a moderate gap severity. These represent persistent threats that, while not as immediately disruptive, can undermine long-term data integrity and trust if left unaddressed.

Overall, the heat map underscores the necessity for a tiered mitigation strategy, prioritizing high-risk, high-gap areas while progressively addressing broader systemic and procedural vulnerabilities. It also visually supports the need for policy reform, capacity development, and infrastructure investment to address these urgent cybersecurity gaps.

5. Conclusion

This study assessed the cybersecurity posture of Philippine aviation using document analysis, regulator-documented case studies, and a transparent likelihood–impact–vulnerability scoring rubric. The results prioritize three critical threats—unauthorized access to air traffic control systems, data breaches in airline reservation platforms, and ransomware on airport networks—driven by monitoring gaps, legacy systems, and uneven policy enforcement. Moderately ranked risks (weak framework implementation; phishing) and under-analyzed insider risks reflect systemic and human-factor weaknesses compounded by underreporting and fragmented inter-agency coordination.

Beyond diagnosis, the study contributes a localization map that operationalizes international frameworks under local constraints: ICAO guidance via formal CAAP–DICT coordination and a centralized incident-reporting portal; phased NIST CSF adoption that elevates Identify (asset inventories) and Detect (continuous monitoring) as baselines; and tiered ISO/IEC 27001 certification pathways scaled to operator capacity. A SWOT–TOWS synthesis converts these into actionable priorities, while a staged AI/ML roadmap (from log normalization and anomaly baselines to supervised classifiers and EDR triage) provides low-cost, on-prem options for intermittently connected environments with KPIs (MTTD/MTTR, precision/recall). Collectively, these measures define a practical path to resilience that aligns governance, technology, and workforce development. Advancing this agenda will require regulatory specificity, sustained investment, and coordinated implementation across regulators, airlines, and airports.

5.1 Limitations and Future Research

This study is limited by its reliance on document analysis, secondary case materials, and qualitative risk modeling, without primary data from regulators, airlines, or airport operators. Although the findings were triangulated with publicly available sources, such as CAAP circulars, the DICT's National Cybersecurity Plan, and documented incidents, the absence of stakeholder interviews or surveys constrains the practical grounding of the recommendations.

Another limitation is the absence of quantitative data, such as incident frequencies and cost estimates, which are not publicly disclosed in Philippine aviation due to underreporting and a lack of formal reporting mechanisms. While structured 1–5 scoring rubrics, adapted from ICAO, NIST SP 800-30, and DICT guidelines, were applied to improve consistency, future studies should integrate quantitative approaches, such as operator surveys and Expected Annual Loss (EAL) modeling, to capture financial and operational impacts more systematically.

Future research should also incorporate primary data to capture on-the-ground perspectives, enabling deeper validation of proposed strategies. In addition, studies using real-time data could provide richer insights into the frequency and nature of cyber incidents in Philippine aviation. Comparative analyses between private and government-operated airport systems may reveal essential differences in resilience, policy enforcement, and infrastructure readiness. These directions would strengthen both the evidence base and the applicability of cybersecurity strategies across the sector.

5.2 Recommendations

To translate the findings into action, regulators, operators, and IT teams should adopt a phased, risk-based program anchored on the localized framework adaptations (Section 4.1.1; Table 3), the risk matrix (Section 4.3), and the AI/ML roadmap (Section 4.3.2). The Civil Aviation Authority of the Philippines (CAAP), in coordination with DICT, should issue aviation-specific rules that mandate baseline NIST CSF Identify/Detect controls (asset inventories, ≥90-day log retention, continuous monitoring), establish a centralized incident-reporting portal with harmonized audits, and implement tiered ISO/IEC 27001 certification pathways (major carriers and hub airports first, then regional operators using simplified templates). Regulators should also require periodic sector-wide exercises and publish common KPIs (e.g., MTTD, MTTR, incident closure rate) to drive accountability.

Airlines and airport authorities should institutionalize periodic risk assessments and penetration tests; upgrade legacy systems with encryption, MFA, PAM/least-privilege, network segmentation, immutable backups, EDR, and SIEM/UEBA; and tighten contractor and portable-media controls within a zero-trust architecture, segmenting ATC/operations enclaves and validating recovery playbooks through joint drills. Insider-risk defenses should include joiner–mover–leaver reviews, access recertification, and measurable phishing programs (lower click rates, higher report rates). Aviation IT teams should execute the three-phase AI/ML roadmap: Phase 1—data readiness and anomaly baselines; Phase 2—on-prem unsupervised pilots (log/network anomaly, UEBA) with human-in-the-loop calibration; Phase 3—supervised phishing classifiers and EDR triage with automated escalation/rollback, governed by drift checks, red-team tests, and rollback procedures. Cross-sector actions include standardizing incident taxonomy, sharing anonymized indicators, upskilling the workforce via role-appropriate certifications, and adopting a quantitative extension (operator surveys plus Expected Annual Loss modeling) to inform risk-based budgeting and evaluate control ROI. Collectively, these measures align governance, technology, and workforce capacity to reduce prioritized risks and strengthen national aviation cyber resilience.

Acknowledgment

The author thanks the Philippine State College of Aeronautics for its academic support and the cybersecurity and aviation experts whose published works informed this study.

References

[1] J. Urban, "Not Your Granddaddy's Aviation Industry: The Need to Implement Cybersecurity Standards and Best Practices within the International Aviation Industry," *Albany Law Journal of Science and Technology*, 2016. [Online]. Available: https://doi.org/10.2139/ssrn.2787476

[2] S. Faye, J. Abdulrahman, R. A. Talb, and R. J. Martin, "Cybersecurity in aviation: A case-based approach to preparedness," *Int. J. Inf. Secur. Cybercrime*, 2024. doi: 10.19107/ijisc.2024.02.03

[3] S. Adhikari, "An analysis of the AIAA aviation cybersecurity framework in relation to NIST, COBIT, and DHS frameworks," in *AIAA Aviation 2020 Forum*, 2020. doi: 10.2514/6.2020-2930

[4] E. Blancaflor, M. M. T. Cortez, D. M. Geneta, N. T. D. Miembro, and C. B. G. Alegre, "Comparative analysis of cybersecurity frameworks utilized by industries in the Philippines," in *Proc. Int. Conf. Conceptual Structures*, 2023. doi: 10.1109/ICCS59700.2023.10335521

[5] N. Kagalwalla and P. P. Churi, "Cybersecurity in aviation: An intrinsic review," in *Proc. 2019 5th Int. Conf. Comput., Commun., Control and Autom. (ICCUBEA)*, pp. 1–6, 2019. doi: 10.1109/ICCUBEA47591.2019.9128483

[6] K. Y. Chai and M. Zolkipli, "Review on confidentiality, integrity, and availability in information security," *J. ICT Educ.*, vol. 8, no. 2, pp. 44–59, 2021. doi: 10.37134/jictie.vol8.2.4.2021

[7] Department of Information and Communications Technology, *National Cybersecurity Plan 2022*, 2017. [Online]. Available: https://tinyurl.com/5fcfm78f

[8] A. Shabtai, Y. Elovici, and L. Rokach, "Introduction to information security," in *Cyber Security for Industrial Control Systems*, Springer, 2012, pp. 1–38. doi: 10.1007/978-1-4614-2053-8_1

[9] S. M. H. Bamakan and M. Dehghanimohammadabadi, "A weighted Monte Carlo simulation approach to risk assessment of information security management systems," *Int. J. Enterprise Inf. Syst.*, vol. 11, no. 4, pp. 41–58, 2015. doi: 10.4018/IJEIS.2015100103

[10] J. Informatika, "Manajemen risiko keamanan informasi menggunakan framework NIST SP 800-30 Revisi 1 (studi kasus: STMIK Sumedang)," *J. Informatika dan Telekomunikasi*, vol. 2, no. 2, pp. 31–40, 2017. doi: 10.30591/JPIT.V2I2.484

[11] J. C. Haass, J. P. Craiger, and G. C. Kessler, "A framework for aviation cybersecurity," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, pp. 132–136, 2018. doi: 10.1109/NAECON.2018.8556747

[12] M. Malatji, S. Von Solms, and A. Marnewick, "Socio-technical systems cybersecurity framework," *Inf. Comput. Secur.*, vol. 27, no. 2, pp. 233–272, 2019. doi: 10.1108/ICS-03-2018-0031

[13] K. Charitoudi and A. Blyth, "A socio-technical approach to cyber risk management and impact assessment," *J. Inf. Secur.*, vol. 4, no. 1, pp. 33–41, 2013. doi: 10.4236/jis.2013.41005

[14] M. Thinyane, "Unpacking the complex socio-technical systems assemblages in cybersecurity," in *Proc. Eur. Conf. Cyber Warfare and Secur.*, 2024. doi: 10.34190/eccws.23.1.2155

[15] A. Baron, R. F. Babiceanu, and R. Seker, "Trustworthiness requirements and models for aviation and aerospace systems," in *Proc. 2018 Integr. Commun., Navig., Surveillance Conf. (ICNS)*, pp. 1B3-1–1B3-10, 2018. doi: 10.1109/ICNSURV.2018.8384831

[16] M. Niraula, "Cybersecurity and interoperability of the aviation safety service ecosystem," in *Proc. 2022 Integr. Commun., Navig. and Surveillance Conf. (ICNS)*, pp. 1–12, 2022. doi: 10.1109/ICNS54818.2022.9771482

[17] G. L. Dillingham, G. C. Wilshusen, and N. Barkakati, "Air Traffic Control: The FAA Needs a More Comprehensive Approach to Address Cybersecurity as the Agency Transitions to NextGen," 2015. [Online]. Available: https://tinyurl.com/bdhs6wsx

[18] G. Dave, G. Choudhary, V. Sihag, I. You, and K. R. Choo, "Cybersecurity challenges in aviation communication, navigation, and surveillance," *Comput. Secur.*, vol. 112, p. 102516, 2021. doi: 10.1016/j.cose.2021.102516

[19] A. A. Elmarady and K. Rahouma, "Studying cybersecurity in civil aviation, including the development and application of aviation cybersecurity risk assessments," *IEEE Access*, vol. 9, pp. 143997–144016, 2021. doi: 10.1109/ACCESS.2021.3121230

[20] E. Ukwandu et al., "Cyber-security challenges in aviation industry: A review of current and future trends," *Information*, vol. 13, no. 3, p. 146, 2022. doi: 10.3390/info13030146

[21] C. A. Viveros, "Analysis of the cyber attacks against ADS-B perspective of aviation experts," 2016. [Online]. Available: https://tinyurl.com/4hmaxtv8
[22] M. Pyzynski, "Cybersecurity of unmanned aircraft systems (UAS)," in *Proc. 2020 Int. Conf. Unmanned Aircraft Syst. (ICUAS)*, pp. 1265–1269, 2020. doi: 10.1109/ICUAS48674.2020.9213922
[23] M. Żmigrodzka, "Cybersecurity – one of the greatest challenges for civil aviation in the 21st century," *Saf. Def.*, vol. 6, no. 2, pp. 33–41, 2020. doi: 10.37105/sd.73
[24] S. Jeon, "Improvement measures for aviation security policies and the security management system against potential in-flight cyber threats," *J. Korean Inst. Commun. Inf. Sci.*, vol. 48, no. 11, pp. 1525–1533, 2023. doi: 10.7840/kics.2023.48.11.1525
[25] C. Nobles, D. Burrell, and T. Waller, "The need for a global aviation cybersecurity defense policy," *Land Forces Acad. Rev.*, vol. 27, no. 1, pp. 19–26, 2022. doi: 10.2478/raft-2022-0003
[26] G. Choudhary, V. Sihag, S. Gupta, and S. K. Shandilya, "Aviation attacks based on ILS and VOR vulnerabilities," *J. Surveill., Secur. Saf.*, vol. 3, no. 1, pp. 27–40, 2022. doi: 10.20517/jsss.2021.17
[27] A. Luoto and M. Hakkarainen, "Cyber resiliency of aircraft systems: A literature review," in *Proc. Eur. Conf. Cyber Warfare and Secur.*, 2024. doi: 10.34190/eccws.23.1.2359
[28] D. Lundberg et al., "On the security of mobile cockpit information systems," in *Proc. 2014 ACM SIGSAC Conf. Comput. Commun. Secur. (CCS '14)*, pp. 633–645, 2014. doi: 10.1145/2660267.2660375
[29] H. Lubbe, R. Serfontein, and M. Coetzee, "Assessing the effectiveness of ADS-B mitigations," in *Proc. Int. Conf. Cyber Warfare and Secur.*, 2024. doi: 10.34190/iccws.19.1.2032
[30] E. Habler, R. Bitton, and A. Shabtai, "Assessing aircraft security: A comprehensive survey and methodology for evaluation," *ACM Comput. Surv.*, vol. 56, no. 4, Art. 96, pp. 1–40, 2023. doi: 10.1145/3610772
[31] A. B. Garcia, R. F. Babiceanu, and R. Seker, "Artificial intelligence and machine learning approaches for aviation cybersecurity: An overview," in *Proc. 2021 Integr. Commun., Navig. and Surveillance Conf. (ICNS)*, pp. 1–8, 2021. doi: 10.1109/ICNS52807.2021.9441594
[32] A. Markel and A. Sanghvi, "Addressing electric aviation infrastructure cybersecurity implementation," United States, 2022. doi: 10.2172/1906953
[33] International Civil Aviation Organization, *Aviation Cybersecurity Strategy*, Oct. 2019. [Online]. Available: https://tinyurl.com/3mb2nevp
[34] International Air Transport Association, *Aviation Cybersecurity*, Version 3, May 2020. [Online]. Available: https://tinyurl.com/4987tuej
[35] National Institute of Standards and Technology, *NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments*, 2012. [Online]. Available: https://tinyurl.com/yc6jw3d4
[36] Cathay Pacific Airways, "Cathay Pacific announces data security event affecting passenger data," Oct. 24, 2018. [Online]. Available: https://tinyurl.com/4e3aj73u
[37] Information Commissioner's Office, "Monetary penalty notice: Heathrow Airport Limited," Oct. 8, 2018. [Online]. Available: https://tinyurl.com/rkux5p7c

Author's Profile

Arthur C. Dela Peña is an Associate Professor at the Philippine State College of Aeronautics (PhilSCA), where he has taught for more than two decades. He currently serves as Program Coordinator for Aircraft Maintenance Technology and Aviation Electronics Technology. His research focuses on aviation maintenance, human factors, sustainability in aviation, emerging technologies, and aviation education. He has authored and presented numerous studies in local and international conferences and has published in peer-reviewed and Scopus-indexed journals. He is also an Air Force Reservist, bringing both academic and practical perspectives to aviation research and education.

How to cite this paper: Arthur Dela Peña, "Cybersecurity in Philippine Aviation: A Multi-Method Evaluation of Vulnerabilities and Mitigation Strategies Through Document Analysis, Case Study, and Risk Modeling", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.15, No.6, pp. 41-53, 2025. DOI:10.5815/ijwmt.2025.06.04