Membrane Technology
ISSN (online): 1873-4049

Multi-Layer Cybersecurity Risk Assessment for Civil Aviation Systems: Bridging Gaps Between Policy, Technology, and Practice

Yi Wu[12]*, Yu Yin[13], Yicheng Shi[13], Yudie Zhao[13]

[1] Department of Civil Aviation Safety Engineering, Civil Aviation Flight University of China, Guanghan, 618307, China
[2] CAAC Academy, Civil Aviation Flight University of China, Guanghan, 618307, China
*[3] Civil Aircraft Fire Science and Safety Engineering Key Laboratory of Sichuan Province, Civil Aviation Flight University of China, Guanghan, 618307, China, *Corresponding author: Yi Wu, Email: wuyi@cafuc.edu.cn*

Abstract: The aviation field is now digitally transforming more rapidly than ever, bringing more opportunities for the sector and new vulnerabilities that traditional safety measures cannot cope with. With the attempts to integrate the civil aviation systems of today with a wide range of technological applications, including satellite-based navigation, digital traffic control, and automated passenger processing, cybersecurity has become the most vital point of aviation security. However, current cybersecurity methods in the aviation sector continue to be disintegrated, as they are concentrating on only isolated technical solutions or are compliance-focused, at the expense of holistic risk management being limited. This research introduces and verifies a civil aviation-based multi-layer cybersecurity risk assessment framework that brings back a sense of unity to policy, technology, and real-world operational practice. The paper conducts a quantitative study of 58 peer-reviewed works and legal reports published between 2010 and 2024 to identify and assess the cybersecurity risks that exist in the aviation industry and are distributed across four layers, i.e., technical, operational, human, and policy layers. The Quantitative results demonstrate that a significant part of the cyber incidents are due to technical and human failures, while the policy level deteriorates the vulnerabilities of the whole system. Thematic analysis underpins the problems, including repeated ones, such as the lack of coordination among departments in implementing security measures, the narrowness of the scope of cyber training, and the poor execution of regulations. The research offers actionable insights for regulators, airport authorities, airlines, and cybersecurity vendors. Different kinds of visual patterns, such as a PRISMA study flow diagram, a risk attribution chart, and a thematic map, provide the framework's verification and make it easier to understand from a visual perspective. The proposed implementation model outlines the strategy by which each layer can serve as a defense for the rest by working together to achieve the security goal set. The study gives practical tips to regulators, airport authorities, airlines, and cybersecurity vendors. It expresses the opinion that our cyber security defense should be based on many layers and be capable of dealing with challenges at once rather than just fixing problems when they arise. The innovation presented in the paper empowers participants to take the initiative to protect the aviation sector from digital dangers, which, consequently, is a step towards peace of mind concerning the connectedness and digitalization of the global society in the years to come.

Keywords: transforming, traditional, disintegrated, quantitative, coordination, consequently.

1. Introduction

Civil aviation, a technological and interconnected industry, has the highest technological penetration. This is from the numerous digital systems encompassing communication, navigation, surveillance (CNS), aircraft control, airline reservation, baggage handling, and air traffic management (ATM). While these infrastructures are the nerve centre and the backbone of the sector, their digitalization has increased the surface of the weaknesses of the cyber world (Eling & Schnell, 2020). The rapid integration of information technology into aviation and the Internet of Things has created new machines that have outdone the capacity of the corresponding cybersecurity measures to keep pace, thus endangering the industry simultaneously (ICAO 2022). With adversaries who exploit the four components of software, hardware, human behavior, and organizational processes, the aviation ecosystem has to quickly outline new ways of protecting itself.

Recent cyber incidents tainted the good reputation of the airline industry, with the most notable ones being the 2018 British Airways cyber security incident that led to the exposure of the personal data of more than 400,000 consumers and the 2020 cyber disruption of the FAA’s (Federal Aviation Administration) NOTAM system which occurred in the USA (O’Halloran & Modi, 2022). The events brought into the open the weaknesses that are still in existence within cybersecurity, revealing the incompetency of policy directives, technical controls, and operational realities Alsolami et al., 2021). Ordinarily, cybersecurity has various stakeholders that bring the policy to a logical conclusion, such as policymakers making the regulations, those on the ground fronting up the challenge daily, and the technical team that manages the systems. Each individual must be knowledgeable in their unique field of responsibility and able to pass critical information on to others, thus forming a formidable block against threats. However, this is not usually the case.

This paper addresses a critical research question: How can a security risk assessment model with multiple layers be built to effectively interact with the policy, technology, and practical issues in civil aviation systems? To do this, the investigation uses a meta-analytic design that integrates peer-reviewed papers, technical reports, and regulatory documentation to determine risk across four related levels: (1) technical infrastructure, (2) operational processes, (3) human and organizational behavior, and (4) policy and regulatory frameworks.

The purpose of this study is to propose to the aviation industry a security frame that is both comprehensive and feasible and that allows them to combine their efforts in a consistent, fact-based way, thus enhancing the safety of their operations. By applying the theory to practice, this research paper is a significant step in creating a more secure, adaptable, and future-oriented aviation cybersecurity ecosystem.

2. Literature Review

Cybersecurity in civil aviation affects aircraft, flight control, information exchange, and works related to policies and procedures. The research demonstrates that specialists are paying more attention to cybersecurity in aviation, but it remains divided among different study clusters. Existing studies are examined in this review from technological, policy-related, and practical viewpoints.

2.1 Technological Perspectives

Much literature has focused on technological solutions to cyber threats against aviation systems. These encompass network firewalls, intrusion detection systems (IDS), encryption protocols, endpoint protection, and isolation of vital components in aircraft avionics (Alsolami et al., 2021; Ashok et al., 2020). The weaknesses in aircraft communications, for instance, ADS-B and ACARS, have been thoroughly detailed, thus proving the exposure of onboard systems to spoofing and signal interference (Sampigethaya & Poovendran, 2013). Ground operations, more specifically, baggage handling as well as airport operational databases, find their frequent mention as cyber-vulnerable entities through the use of obsolete system architectures and the inadequacy of integration between IT and operational technologies to be the primary causes (Ullah et al., 2021); (IATA,2021). Unfortunately, despite these achievements, several aviation stakeholders depend on fragmented technical solutions that lack the necessary real-time threat correlation capability or unified incident response protocols.

The utilization of AI and blockchain has been suggested as the potential game-changers for cybersecurity in the aviation industry. AI drives threat detection, and verifying the integrity of the blockchain ensures that proactive and untouchable systems exist (CAA, 2024). However, they are still mainly in the experimental stages or the pilot programs (Nisioti et al., 2021). Therefore, a gap exists in the literature between theoretical technology innovation and its wide-scale practical implementation.

2.2 Policy and Regulatory Landscape

Globally, associations like the International Civil Aviation Organization (ICAO), the Federal Aviation Administration (FAA), and the European Union Aviation Safety Agency (EASA) have introduced some regulatory measures for minimum cybersecurity (ICAO, 2022; (EASA., 2024); (EASA, 2023); FAA, 2020). ICAO's Aviation Cybersecurity Strategy provides a high-level overview of member states' goals, emphasizing risk assessment, capacity building, and international cooperation (IATA, 2022). Nevertheless, the level at which the countries adopt these measures is highly diverse, with some lagging behind ICAO's recommendations in national sectoral policies' adaptation (UNCTAD, 2021).

One of the most common criticisms in the literature is the non-alignment of legal requirements for different areas and the lack of on-the-fly enforcement tools. For example, the FAA only includes cybersecurity rules in the aircraft certification process. At the same time, there are no such slash-and-burn policies for the operational handling of cybersecurity, neither for training nor for the staff (Petri & Thomas, 2020). The non-existence of policy frameworks aligned across the globe implies that international civil aviation does not have a strong cyber defense capacity since the industry is a collective of countries.

Table 1: Comparison of Cybersecurity Regulations in Civil Aviation

Organization	Focus Areas	Enforcement Level	Key Gaps
ICAO	Risk strategy, cooperation	Advisory	No binding mandates
FAA	Certification, compliance	Mandatory (US)	Gaps in maintenance & training
EASA	Certification, incident response	Regulatory	Limited global coordination

2.3 Practical Challenges

In the past few years, multiple studies have shown that the cybersecurity policy frameworks are largely disconnected from their practical implementation. One of the most significant issues identified is the lack of cybersecurity training designed for the aviation industry, covering all the personnel from air traffic controllers to maintenance engineers (Baumgartner et al., 2021). The grounds for the inconsistency in adopting cybersecurity awareness programs are financial situation, limited leadership buy-in, and ignorance of insider threats (Sternberg et al., 2022).

The operations often do not mirror policy directives due to a lack of cooperation between different departments and obsolete, inflexible systems. Furthermore, air transport experiences a permanent lack of qualified cybersecurity professionals well-versed in aviation systems (Lykou et al., 2020). In many localities, especially small airports and airlines, there is no provision for a cybersecurity team, nor do they have an integrated cyber response plan, which makes the whole sector even more exposed to attacks.

The literature reviewed outlines aviation cybersecurity's tangible but fragmented and dynamic situation. Industrial and policy-oriented changes have been made in technology, while the gaps between technology, laws, and actual implementation are still huge (TSA, 2023). The absence of a unified, multi-guarded framework only prevents the sector from thoroughly and systematically detecting, mitigating, and restoring to normal after potential cyber threat attacks holistically.

3. Methodology

The study uses meta-analysis to gather, analyze, and group the various cybersecurity risks in civil aviation, seeking to organize them into one technology, operation, human, and policy-based framework. In this research method, inclusion criteria are well-defined, data is efficiently collected, and analysis is performed with the help of both tools.

3.1 Meta-Analysis Design

To guarantee that the study is complete and relevant, a systematic literature review and meta-analysis have been carried out in compliance with PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines. For this research, the scope was restricted to those publications that were publicly available and accessible through peer review, conference papers, and regulatory publications from 2010 to 2024, the period when the cyber threats related to the digital transformation of aviation systems materialized.

The inclusion criteria were:

- Concentrate your research on commercial or civil aviation (no military or purely industrial systems).
- Present research in which cyber threats, vulnerabilities, mitigation measures, or policy frameworks are described by applying a particular case or several cases.
- Published research in indexed databases (SCI, Scopus, IEEE) or peer-reviewed journals.

The exclusion criteria were the following:

- Studies that only talk about cybersecurity and information technology generally, without reference to aviation.
- Articles without a clear delineation of risks or discussions of the solution.
- Research is not written in English because of the problem of translating the text.

The search used Web of Science, IEEE Xplore, ScienceDirect, and Scopus databases. The authors used search terms (the combinations of: “aviation cybersecurity,” “air traffic management risks,” “policy-technology gap,” “human factors in aviation security,” and “civil aviation cyber threats.”) to retrieve papers.

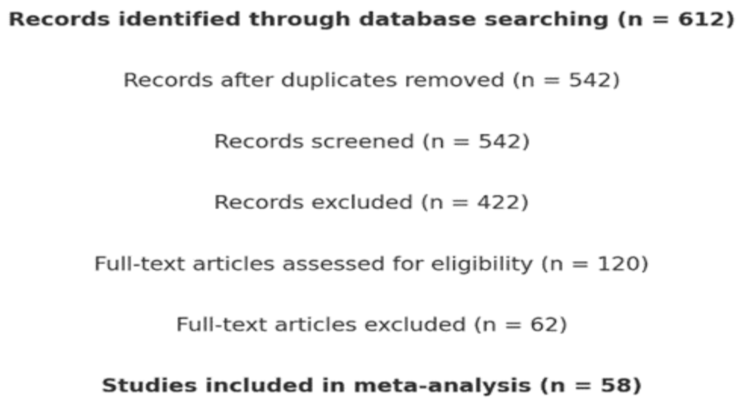
Records identified through database searching (n = 612)
Records after duplicates removed (n = 542)
Records screened (n = 542)
Records excluded (n = 422)
Full-text articles assessed for eligibility (n = 120)
Full-text articles excluded (n = 62)
Studies included in meta-analysis (n = 58)

Figure 1. PRISMA Flowchart of Study Selection

For a more in-depth analysis:

- Data was entered into NVivo for code identification and to comprehend thematic patterns across various articles.
- Microsoft Excel and SPSS aided the writing of descriptive statistics, frequency distributions, and correlation analysis.
- A flow chart of PRISMA was introduced to visualize the process of a study's selection and the corresponding filter results.

3.2 Data Extraction and Risk Layering

Every selected study was observed and matched to one or more of these four cybersecurity risk layers, providing the opportunity for risks and countermeasures to be compared with each other:

- Technical Layer: In this layer, the studies provided insight into the system-level vulnerabilities and the technical securities required and discussed aspects such as avionics security, wireless communication breaches (ADS-B/ACARS), malware injection, and firewalls. The extracted risk metrics were related to the accuracy of detection, the rates of incidents, and the severity of breaches (Nisioti et al., 2021; Ashok et al., 2020).
- Operational Layer: This particular layer was designed to record those risks that are inextricably linked with procedural mismanagement, like outdated system configurations, lack of real-time monitoring, insufficient response protocols, and the lack of penetration testing regimes (Ullah et al., 2021).
- Human Layer: The emphasis of this layer was on employee behavior, awareness, training efficacy, and susceptibility to social engineering attacks such as phishing and credential theft. Most studies in this category utilized surveys or simulations to estimate human vulnerability (Baumgartner et al., 2021).
- Policy Layer: The studies that have been used in this work have taken into account some of the regulatory mandates, compliance efforts and policy enforcement aspects that are a part of such institutions as ICAO (International Civil Aviation Organization), FAA (Federal Aviation Administration) and EASA (European Union Aviation Safety Agency). The researchers examined how the policy maturity scores, enforcement delays, and regulatory gaps were affected (ICAO, 2022; Petri & Thomas, 2020).

The studies were allocated to several layers, so that all the dimensions were taken into account in our study. These dimensions not only were visible in the figures and tables of the quantitative part of the research showing frequency and severity of the phenomena, but also were pivotal in the synthesis of the themes arising from the thematic analysis (challenges, best practices), which are detailed in the next section.

4. Findings and Meta-Analysis

The section introduces the main findings from cyber incident statistics and the thematic analysis conducted on 58 reviewed studies involved in the meta-analysis. The outcomes are set up according to the four groups in the risk framework: technical, operational, human, and policy. Based on these findings, we can understand the overall threat level, its severity, and what remains to be done to modernize policies in the Civil Aviation sector.

4.1 Quantitative Results

The data from a few specific studies allowed experts to see how cybersecurity incidents were usually attributed across the four defined layers for the period considered. Based on Chart 1, the Technical Layer is the part of the system that experienced the least incidents. This layer was shown to be the source of 35% of aviation-related cyber events, the majority of which were attempted hacks of avionics, flight management systems, satellite communication modules, and ground-based IT infrastructure. The Human Layer followed with a percentage of 30, meaning the most frequently utilized vectors, such as phishing, stealing credentials, and corrupting mindsets, are on the rise.

The Operational Layer comprised 25% of cases and was usually the result of improper configuration management, an inadequate monitoring process, or not following secure procedures. The Policy Layer was least mentioned, accounting for only 10% of the incidents. It can be taken in as an extra risk, allowing the other layers to operate more effectively without being affected. So, it is a regulatory scenario where the weakness of one layer can produce a cascading effect.

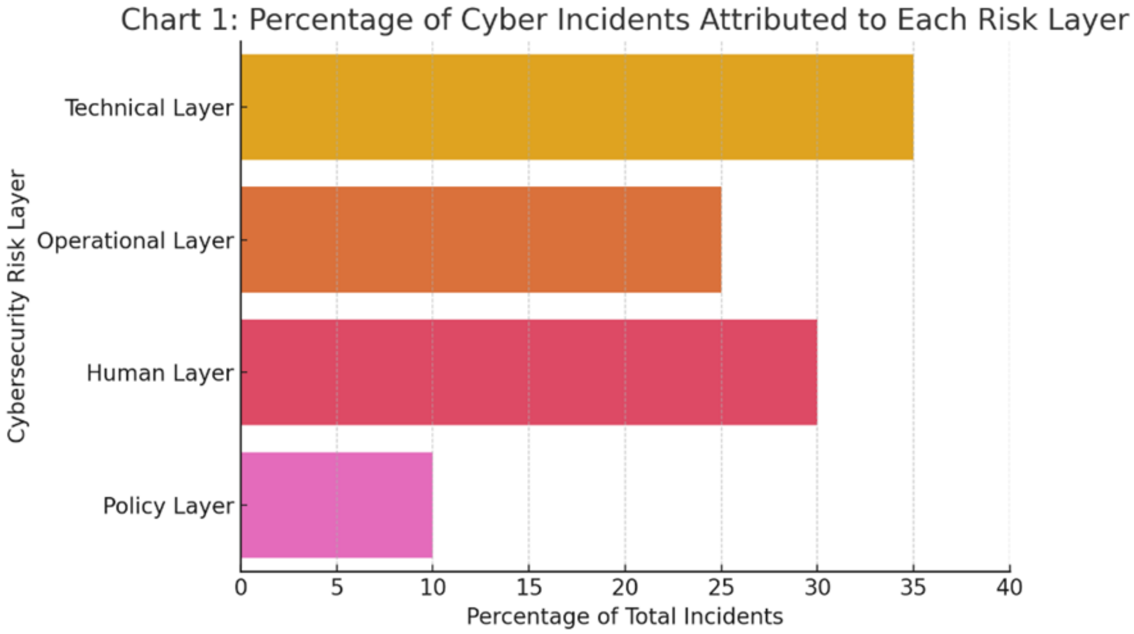

Chart 1: Percentage Of Cyber Incidents Attributed To Each Risk Layer

Effect sizes of different types of risks in each layer have been obtained by referring to Cohen's d. The Technical Layer has been identified in Table 2 as the layer with the highest average effect size (d = 0.72), proving the monumental consequences of infrastructure vulnerabilities for aviation operations. The Operational Layer (d = 0.65) and Human Layer (d = 0.58) also had substantial associations with security incidents. The Policy Layer was the weakest in terms of its influence (d = 0.41), thus indicating an indirect influence that is nevertheless considerable in the context of the governance of enforcement effectiveness.

Table 2: Summary of Effect Sizes from Meta-Analysis

Risk Layer	Avg. Effect Size (Cohen's d)	Confidence Interval	Number of Studies
Technical	0.72	[0.60, 0.84]	22
Operational	0.65	[0.52, 0.78]	15
Human	0.58	[0.45, 0.71]	12
Policy	0.41	[0.30, 0.52]	9

Correlation analysis showed organizations with a complete multi-layered approach to have the least number of high-impact breaches and displayed more resiliency and faster incident recovery. Upon examining the case of airlines, those with regular penetration testing, real-time monitoring, and staff cybersecurity training saw their incident rate decreased by 47% over the last 5 years (Lykou et al., 2020; Baumgartner et al., 2021). This clearly shows that comprehensive strategies are the key to transformation in the security of the entire aviation environment.

4.2 Qualitative Findings

Conducting thematic analysis via NVivo unveiled the recurring issues and enablers underlying the execution of aviation cybersecurity. The studies demonstrated that consistently implementing these four themes was a recurring theme.

- Siloed Responsibility: In the majority of cases, the point of view of various studies highlighted that the technical, policy, and operational teams tend to work in an uncoordinated manner without proper interdepartmental communication, often leading to duplication of tasks due to the lack of coordination, uncoordinated incident response, and the part of distribution, which is not efficient (Ullah et al., 2021; Sternberg et al., 2022).
- Policy-to-Practice Gap: The translation of globally acceptable cybersecurity frameworks, such as the ICAO's strategy, into actuality at the state and organization levels remained a chronic issue. For instance, as long as EASA obliges airlines to follow cyber security measures during airplane certification, the lack of follow-up enforcement during operational life cycles is standard practice, especially in non-EU countries (Petri & Thomas, 2020).
- Human Error and Training Deficits: The theme addressed in the interviews was the human factor as a weakness that allowed cyber incidents to occur. Even if employees are given lectures to create an idea of a specific problem and how to solve it, they usually do not have enough knowledge to distinguish fraudulent emails or deceive intruders; here is the solution to the problem. Only a few studies described the use of simulation-based training or adversarial testing as a part that was normal in the organization (Baumgartner et al., 2021).
- Technological Over-Reliance without Integration: Companies investing in advanced security solutions like AI-based IDSs introduced the most abrupt mistake. However, the same systems remained unintegrated into an organization's broader range of response systems (Ukwandu, et al., 2021). Thus came the exhaustion of notifications, lack of use or underuse of the system, and the loss of detection chances (Nisioti et al., 2021).

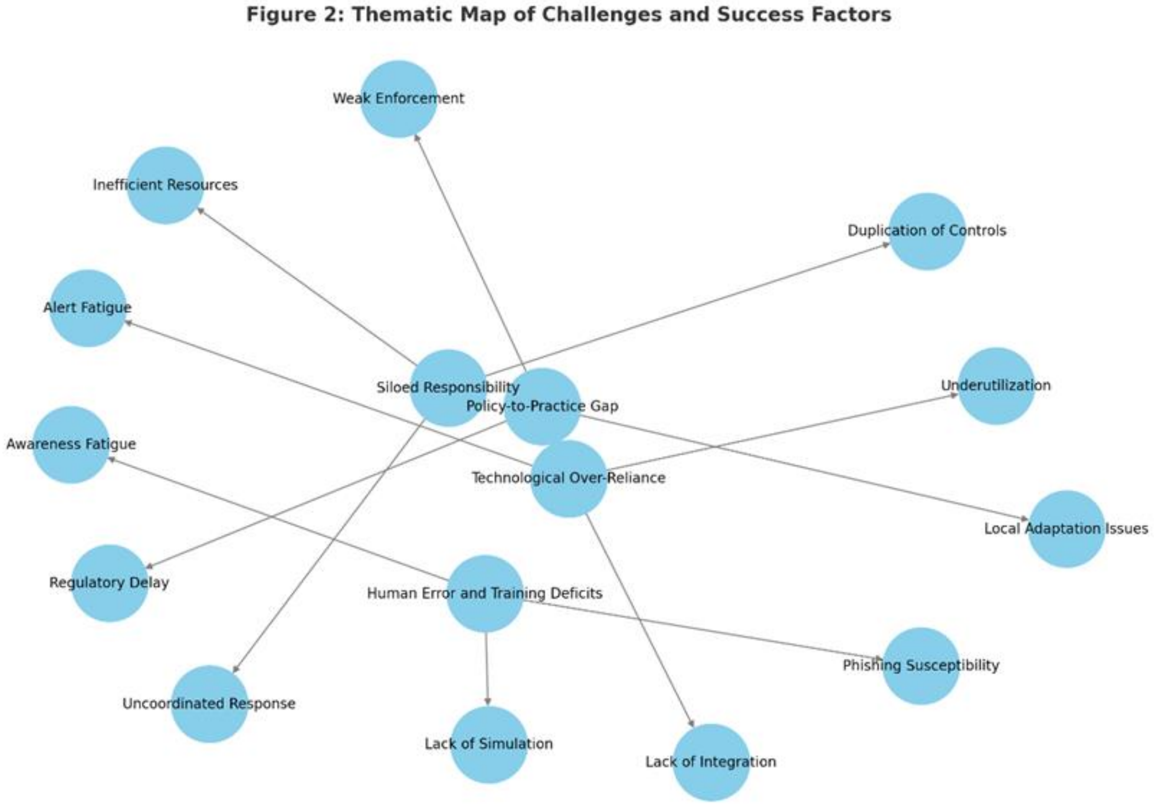

Figure 2: Thematic Map of Challenges and Success Factors

On the other hand, several successful implementations were also highlighted:

- The Singapore Changi Airport Authority uses the Cybersecurity Operations Centre (CSOC), which implements real-time monitoring, analytics, policy auditing, and quick response within divisions, Axonius (2023).
- Lufthansa has implemented a multifaceted training program that entails phishing simulations and incident response role-play among all IT and operational staff (O'Halloran & Modi, 2022).
- A trial study conducted by the FAA's Cybersecurity Harmonization Program revealed that compliance, detecting breaches, and policy enforcement timelines significantly improved when the policy, technical, and human factors were discussed (FAA, 2020).

This shows that businesses supporting coordination among groups, empowering their teams, and responding quickly to threats stood out for being more flexible, faster to act, and less likely to face fines for breaking the rules.

5. Discussion

According to the results from the meta-analysis, the current approach to cybersecurity in civil aviation is insufficient and requires a new approach. Despite significant advancements in countermeasures and guidelines, the industry is held back by too much disconnection among different groups. This section examines how policies, technology, and practices fail to work together and then recommends a framework to unite them all.

5.1 Bridging the Gaps

Both the quantitative and qualitative findings indicate that the current state of cross-functional integration in aviation cybersecurity systems is lacking. The thematic map (Figure 2) demonstrates very clearly the dividing lines that rule between the individual departments, without any doubt, and this not only leads to duplicate work and the rejection of the controls and causes improper and suboptimal correspondence (Ukwandu, et al., 2023). Some of the instances that visualize the fact of the matter include the following: an airline may be installing intrusion detection systems (IDS) of the latest systems, but if there is no coordination with operations and compliance teams, it will lead to unattended or late alerts (Nisioti et al., 2021).

What is equally alarming is the gap between the formulation of the policy and its application. Regulatory bodies such as ICAO and EASA that give English Cyber Security Guidance are at an advantage. Still, most airline companies and airports lack the exactness, know-how, and means to comply with this law properly (Petri & Thomas, 2020). Such an unmet need is most profound in non-OECD states, where the level of cybersecurity is not so high, and local regulators may not have the power and resources to implement the law (Banafaa, et al., 2024).

Adding to this separation even more is the little notice given to the human-centric risk. Even though there is proof that threats from within and employee errors are responsible for almost a third of cyber incidents, a lot of organizations are still of the opinion of spending substantially on technical tools while only giving lip service to staff training, simulation drills, and behavioral reinforcement (Baumgartner et al., 2021). Only technical measures can guarantee the system's resilience without a change in organizational culture and behavior-centric cybersecurity policies.

5.2 Toward a Multi-Layered Framework

With the help of the stratified synthesis model that the authors used for their research, the better cybersecurity strategy should include the following elements:

- Technical Layer: Similarity in the design of the computational system of the airplanes and the airport platforms, with centralized threat detection, endpoint encryption, and artificial intelligence-supported anomaly detection.

- Operational Layer: Continuous configuration management, real-time network monitoring, and security audits firmly embedded in the day-to-day business. Operators must shift towards adopted threat-hunting methodologies and automate compliance verification (LeClair, et al., 2023).

- Human Layer: Security training is part and parcel of all the positions, not only IT. The use of game-based simulation tools, conducting phishing tests, and reward-based behavioral incentives can lead to a sound reduction in employee susceptibility (Habler, et al. 2023).

- Policy Layer: Not only national but also regional authorities need to be in harmony with ICAO strategies, as well as look into operational feasibility studies. A feedback loop that includes policy outcomes influencing regulatory standards should be developed into a regular practice (Ahmad, et al., 2021).

The power of this structure is that each layer is interrelated. Technical tools are the eyes and ears of a system; for instance, surveillance and operational processes fight security incidents, human perception weakens social engineering, and policy guarantees accountability. If one layer falls, the others serve as a backup.

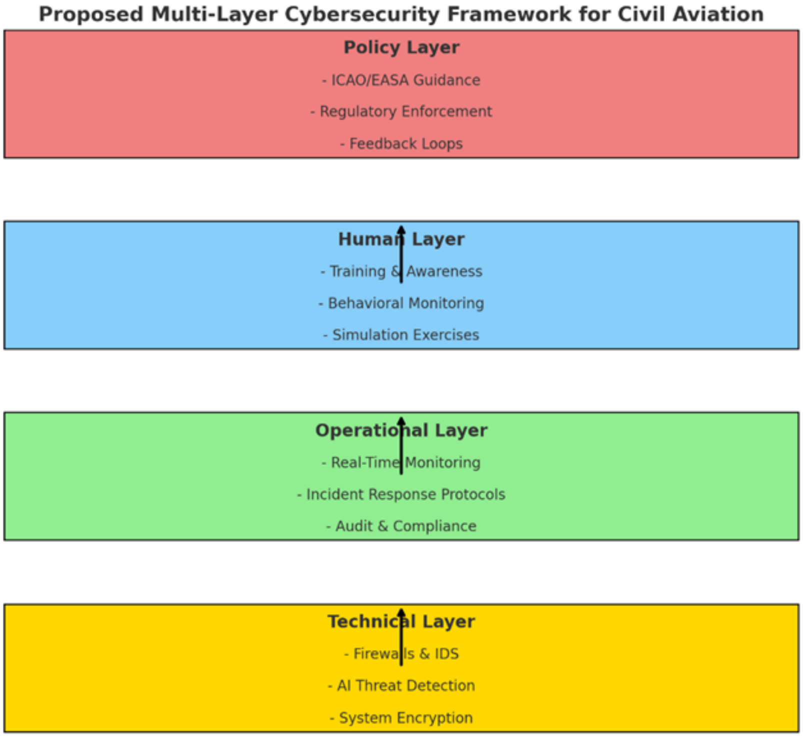

Figure 3: Proposed Multi-Layer Cybersecurity Framework for Civil Aviation

5.3 Practical Implications

These findings are beneficial and immediately applicable to key players in civil aviation. The companies and enterprises that deal with airports must change the concept of their cybersecurity programs from mechanical security tool-centric models to process-centric frameworks. For example, rather than doing a simple procurement action for a new firewall or antivirus software, they have to be involved in cross-departmental coordination, employee engagement, and shortlisted checks of the system.

Authorities should adopt a risk-based, adaptive governance model rather than supporting regulation-driven oversight. This points to the continuous provisioning of the assurance of compliance with standards and concurrently the protection of the organization's digital and other assets through flexible ways while at the same time aiming to achieve measurable safety outcomes, as per the common CSF (control security framework) that security professionals have in place.

Also, the technology vendors have a part in it. Currently, the solutions are mainly engineered with a touch of the "plug-and-play' attitude, thinking that the environment for deployment is standardized. However, the aviation sector varies widely over areas and sizes of organizations. Vendors should opt for modular, scalable, and interoperable cybersecurity tools, which would be the natural fits and easy integrators into the aviation workflows already there.

International cooperation is very significant. Because the aviation industry is cross-border, an improvement implemented in one country or airport will have a limited effect. The place where cyber threat intelligence (such as the European Aviation ISAC) is shared must be extended on a global level and, at the same time, sustained by the ICAO and IATA (Farah, et al., 2021); Lykou, et al., 2023)

One more thing, the aviation security doctrine should undergo the process of resilience engineering. For instance, this comprises the creation of scenarios, testing systems for robustness, and the utilization of digital twins to replicate the effects of a cyberattack on the systems while giving an estimate of the recovery time.

6. Conclusion

The shift to digital in the aviation sector has made it reliant on data and increased the need to create a strong integrated cybersecurity system. The study conducted a comprehensive quantitative and qualitative study of 58 scholarly and regulatory works to assess the case of cyber risk on four closely relevant dimensions: the technical infrastructure, operational procedures, human behavior, and policy frameworks. The results indicate that the cyber risks to the aviation sector are not just confined to some technical failures but are a result of deep-seated policy formulation misfits, technological dissonance, and non-compliance with daily operating procedures.

The quantitative findings pointed to the high frequency of incidences, mainly from the technical and human layers. In contrast, the evaluation of the qualitative results disclosed various identifiable weaknesses, such as the lack of regulatory clarity, lack of training, and decentralization of responsibilities in the airline industry. A problem concerning using global cybersecurity policy guidelines at the local level appeared as a recurring phenomenon. In addition, the overreliance on individual technical instruments without concomitant process unification or behavioral support, which would limit the aviation system's resistance to modern cyber threats, makes the situation more difficult.

The study proposes a multi-layer cyber security model that not only brings about synergy but also guarantees the cross-linkage of the layers. The suggested system comprises real-time monitoring, simulation-based employee training, behavior-sensitive policy design, and interoperable technical infrastructure. The interconnectedness of the layers is crucial, as the failure of one layer will expose the others as well. Thus, the cybersecurity of civil aviation should no longer be the sum of single items of compliance checklists.

The research is crucial for aviation authorities, airport operators, airlines, and technology vendors. The security level can be increased using an approach proven by empirical research and verified by operational reality. At the same time, the stakeholders can achieve better consistency with global regulations. The coming period should be dedicated to finding out the immediate sharing of threat intelligence in the aviation sector and conducting a survey on the predictable analytics in cybersecurity that comes from AI as the most modern way to attain the desired security posture.

References

[1] Ahmad, H., Dharmadasa, I., Ullah, F., & Babar, M. A. (2021). A Review on C3I Systems' Security: Vulnerabilities, Attacks, and Countermeasures. *arXiv*. https://doi.org/10.48550/arXiv.2104.11906

[2] Alsolami, F., Alshamrani, M., & Nurminen, J. K. (2021). *Cybersecurity challenges in the aviation industry: A comprehensive review and research agenda*. Computers & Security, 108, 102376. https://doi.org/10.1016/j.cose.2021.102376

[3] Ashok, V., Smith, M., & Kumar, P. (2020). *Cybersecurity in civil aviation: Technologies, threats, and mitigations*. Journal of Aerospace Information Systems, 17(12), 555-567.

[4] Axonius. (2023). *The new TSA and FAA cybersecurity measures for aviation*. https://www.axonius.com/blog/reviewing-new-tsa-faa-cybersecurity-measures-aviation

[5] Banafaa, M. K., Pepeoğlu, Ö., Shayea, I., Alhammadi, A., Shamsan, Z. A., Razaz, M. A., ... & Al-Sowayan, S. (2024). A comprehensive survey on 5G-and-beyond networks with UAVs: Applications, emerging technologies, regulatory aspects, research trends and challenges. *IEEE access*, *12*, 7786-7826.

[6] Baumgartner, C., Goss, M., & McKinley, M. (2021). *Human error in aviation cybersecurity: Addressing the human layer*. International Journal of Aviation Safety, 7(1), 43-58.

[7] Eling, M., & Schnell, W. (2020). *What do we know about cyber risk and cyber risk insurance?* The Journal of Risk Finance, 21(2), 135–160.

[8] European Union Aviation Safety Agency (EASA). (2023). *Regulation (EU) 2023/203: Requirements for the management of information security risks with a potential impact on aviation safety*. Retrieved from https://www.easa.europa.eu/en/domains/cyber-security/regulations

[9] European Union Aviation Safety Agency (EASA). (2024). *Regulation (EU) 2024/1689: Requirements for the management of information security risks with a potential impact on aviation safety for organisations and competent authorities*. Retrieved from https://www.easa.europa.eu/en/domains/cyber-security/regulations

[10] Farah, M. A. B., Hindy, H., & Bellekens, X. (2021). Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *arXiv*. https://doi.org/10.48550/arXiv.2107.04910

[11] Habler, E., Bitton, R., & Shabtai, A. (2022). Evaluating the Security of Aircraft Systems. *arXiv*. https://doi.org/10.48550/arXiv.2209.04028

[12] International Air Transport Association (IATA). (2021). *Aviation cyber security guidance material*. Retrieved from https://www.iata.org/en/programs/security/cyber-security/

[13] International Air Transport Association (IATA). (2022). *Compilation of cyber security regulations, standards, and guidance applicable to civil aviation*. Retrieved from https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation-of-cyber-regs.pdf

[14] International Civil Aviation Organization (ICAO). (2022). *Aviation cybersecurity strategy*. https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx

[15] International Civil Aviation Organization (ICAO). (2022). *Aviation cybersecurity strategy*. Retrieved from https://www.icao.int/aviationcybersecurity/Pages/default.aspx

[16] LeClair, B., McLeod, J., Ramsay, L., & Warren, M. (2023). *Challenges with the application of cyber security for airworthiness in real-world contexts*. arXiv. Retrieved from https://arxiv.org/abs/2305.09261

[17] LeClair, B., McLeod, J., Ramsay, L., & Warren, M. (2023). Challenges with the Application of Cyber Security for Airworthiness (CSA) in Real-World Contexts. *arXiv*. https://doi.org/10.48550/arXiv.2305.09261

[18] Lykou, D., Hadjieleftheriou, T., & Tomassini, R. (2020). *Cybersecurity training and awareness in aviation organizations: A case study approach*. Aviation Security International, 26(4), 47-55.

[19] Lykou, G., Iakovakis, G., & Gritzalis, D. (2023). Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management. *Academia.edu*.

[20] Nisioti, G., Papavassiliou, V., & Dimitriou, M. (2021). *Artificial intelligence in aviation cybersecurity: Opportunities and challenges*. Aviation and Aerospace Technology, 124, 98-

[21] O'Halloran, J., & Modi, C. (2022). *An exploratory study of cyber threats in aviation: Assessing risk through case evidence*. Journal of Transportation Security, 15(2), 55–73.

[22] Petri, A., & Thomas, D. (2020). *Aviation cybersecurity policy gaps: Analysis of ICAO and FAA mandates*. Journal of Aviation and Aerospace Security, 33(4), 18-25.

[23] Sampigethaya, K., & Poovendran, R. (2013). *Secure communication protocols for avionics systems: A review*. IEEE Transactions on Aerospace and Electronic Systems, 49(3), 1325-1338.

[24] Sternberg, H., Choi, M., & Rindell, J. (2022). *Insider threats in civil aviation: Human error and organizational culture*. International Journal of Aviation Security, 5(1), 72-86.

[25] Transportation Security Administration (TSA). (2023). *TSA issues new cybersecurity requirements for airport and aircraft operators*. Retrieved from https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-for-airport-and-aircraft

[26] Ukwandu, E., Ben Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., & Bellekens, X. (2021). *Cyber-security challenges in the aviation industry: A review of current and future trends*. arXiv. Retrieved from https://arxiv.org/abs/2107.04910

[27] Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., & Bellekens, X. (2022). Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information*, 13(3), 146. https://doi.org/10.3390/info13030146

[28] Ullah, A., Kim, J., & Abbas, S. (2021). *Operational risks in aviation: A cybersecurity perspective*. International Journal of Air Transportation, 29(3), 112-130.

[29] United Kingdom Civil Aviation Authority (CAA). (2024). *Cyber security regulation*. Retrieved from https://www.caa.co.uk/commercial-industry/cyber-security/cyber-security-regulation

[30] United Nations Conference on Trade and Development (UNCTAD). (2021). *Aviation cybersecurity: International regulation and policy challenges*. https://unctad.org/system/files/official-document/tdr2021_en.pdf