International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Cybersecurity as an extension of safety management in business aviation

Ahamba-Olorunsola Adaku Blessing *

Embry-Riddle Aeronautic University, Florida, United States of America.

International Journal of Science and Research Archive, 2024, 13(01), 3612-3617

Publication history: Received on 16 September 2024; revised on 21 October 2024; accepted on 29 October 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.13.1.2054

Abstract

As data-driven networks reshape business aviation, the intersection of cyber threat and operational safety is now a direct concern. The following paper posits that cybersecurity must be integrated as a logical extension of Safety Management Systems (SMS) within business aviation operators. Leveraging the latest scholarly work (e.g., Dave et al., 2022; Florido-Benítez, 2024) and recognized international best practices, we align evidence that commonly deployed aviation technologies such as electronic flight bags (EFBs), datalink connectivity, maintenance data pathways, supply-chain applications, and the interfacing of airport and ATM systems, embed cyber risk channels that could have safety implications. We complement this analysis with a quantitative survey administered to 120 business aviation practitioners, obtaining results on the depth of SMS-cyber convergence, the implementation of protective controls, prior incident exposure, the breadth of training, and perceived implementation barriers. The results indicate that, while the industry broadly acknowledges the interdependence of cyber and safety domains, the integration into SMS mechanisms remains patchy: multi-factor authentication and EFB platform hardening have achieved widespread conformity, yet security operations centre (SOC) oversight, security incident and event management (SIEM) deployment, and supplier cyber vetting remain insufficiently embedded. The paper thus advances operational guidance for systematically weaving cyber risk into the SMS architecture, encompassing hazard identification, risk acceptance, performance monitoring, and safety training, while underscoring measures that deliver a material reduction in residual risk tailored to the structure and operations of business aviation. (Dave et al., 2022; Florido-Benítez, 2024).

Keyword: Cyber security; Cyber Risk; Electronic Flight Bags; Safety Management Systems

1. Introduction

Digitalization has revolutionized the operational landscape of business aviation, from flight planning and performance apps on electronic flight bags to maintenance telemetry, fleet scheduling, and real-time connectivity between airborne and ground nodes. While this interconnected architecture streamlines efficiency, it also enlarges the attack surface; malicious actors can now compromise flight-related data to erode confidentiality, integrity, or availability, ultimately translating into safety problems (Dave et al., 2022). Meanwhile, modern attacker ecosystems including criminal syndicates and state-sponsored groups systematically target aviation stakeholders through phishing, ransomware, and compromises of third-party suppliers (Florido-Benítez, 2024). If cybersecurity domains operate outside the safety management system (SMS), critical blind spots can arise; by union instead treat threats across the SMS's core four pillars (policy & objectives, risk management, assurance, and promotion), aviation stakeholders synchronize risk management with the established risk-based decision-making processes that underpin system safety (Lykou, Anagnostopoulou, & Gritzalis, 2019; Dave et al., 2022).

Purpose and contribution. This paper (i) consolidates the state-of-the-art scholarship on aviation cyber threats, focusing on systems that are specific to business aviation; (ii) advances a safety management system framework that

* Corresponding author: Ahamba-Olorunsola Adaku Blessing

incorporates cyber risk; and (iii) examines the current level of integration by administering a quantitative survey of personnel across the business aviation sector.

2. Literature Review

2.1. Threat landscape and cyber-to-safety pathways

Surveys conducted on aviation communication, navigation, and surveillance (CNS) systems and their ground-support infrastructure continue to catalogue documented security weaknesses (Dave et al., 2022). Identified attack pathways range from deliberate signal jamming or spoofing to exposing specific protocol deficiencies such as ADS-B integrity, along with competition of external, interconnected maintenance or operational management interfaces. These attack classes, if pursued, can lead to diluted situational awareness or deliberate procedural deviation, potentially resulting in safety-critical incidents (Dave et al., 2022). Upstream investigations, in concert with the vulnerability assessments, align attack typologies and actor motivations, revealing a heterogeneous landscape extending from ethically-oriented hackers to state or sponsored adversaries and organized crime. Each category manifests a distinct computational or operational attack pattern, favouring particular on-board, carrier, and/or fixed-base terminal characteristics of the commercial and business jet sectors (Florido-Benítez, 2024).

The acceleration of cloud-based and IoT functionality within airports and ATM infrastructure is producing a visibly "smart" operational layer; empirical investigations now document inconsistent deployments of corresponding cybersecurity practices and conspicuous resilience shortfalls within mission-critical systems (Koroniotis, et.al., 2020). For business aviation fleets, reliance on fixed-base operator (FBO) services and the attendant airport domains makes the smart operational interfaces a potential import pathway for malicious codes or fragmented intrusion vectors (e.g., stealthy lateral movement through a compromised Wi-Fi overlay or secondary ground-handling control platform). This technical vulnerability, in tandem with external supply continuity, underlines the necessity of expanded third-party cyber governance as a persistent and substantive element of the operational safety management system (Lykou et al., 2019).

2.2. From security to safety: integrating with SMS

The body of current research continues to underscore the necessity of leveraging risk-based frameworks together with continuous monitoring technologies chiefly adapted SOC and SIEM capabilities—so that cyber threats can be promptly identified, countered, and later examined; these activities mirror the assurance loops integral to any Safety Management System (Marisa & Coetzee, 2024). Comprehensive comparative reviews further advocate that cyber hazards be explicitly modeled in parallel with pre-existing operational threats, urging the amalgamation of both domains into single workflows covering incident reporting, formal investigation, and persistent safety action tracking (Marisa & Coetzee, 2024).

Synthesis. The converging evidence now affirms that cyber hazards exceed conventional information security boundaries and can precipitate or amplify operational safety events. Embedding cybersecurity controls into extant SMS frameworks is thus not only a coherent cognitive alignment but a pressing operational requirement.

3. Methodology

3.1. Research design

A quantitative, cross-sectional online survey was administered to professional cohorts within business aviation. The design aimed to measure (1) the extent of cyber-SMS integration, (2) the occurrence of prescribed protective measures, (3) historical incident exposure, (4) training frequency, and (5) participant-identified barriers.

3.2. Population and sample

Target respondents comprised flight operations, maintenance/airworthiness, safety managers, operations control, and IT/security personnel across the business aviation sector, including Part 135/charter, corporate flight departments, and FBO-affiliated operators. N = 120 valid responses was achieved, reflecting completed questionnaires.

3.3. Instrument

A structured questionnaire featuring closed-ended items gathered demographic data and organizational cybersecurity practices. The principal variables of interest were as follows:

Integration: "Are cybersecurity hazards formally documented in the SMS hazard registry and risk assessments?" (Yes/No).

Controls: Adoption (Yes/No) of multi-factor authentication (MFA) for privileged accounts, electronic flight bag (EFB) hardening and baseline, 24/7 security operations center (SOC) or security information and event management (SIEM) monitoring, and supplier cybersecurity due diligence.

Incidents: "Has your organization experienced a cyber incident impacting operations in the past 12 months?" (Yes/No).

Training: Reporting of frequency for flight, operations, and maintenance personnel (Quarterly, Semiannual, Annual, or None).

4. Results

Table 1 Respondent roles (N = 120)

Role	Frequency	Percentage (%)
Flight crew/Dispatch/OCC	34	28.3
Maintenance/Continuing Airworthiness	26	21.7
Safety Manager/Quality	22	18.3
IT/Security	18	15.0
Operations Management/Admin	20	16.7
Total	120	100.0

The sample covers all core business-aviation functions, with the largest group from flight operations. This mix supports perspectives across the SMS and cyber control environment.

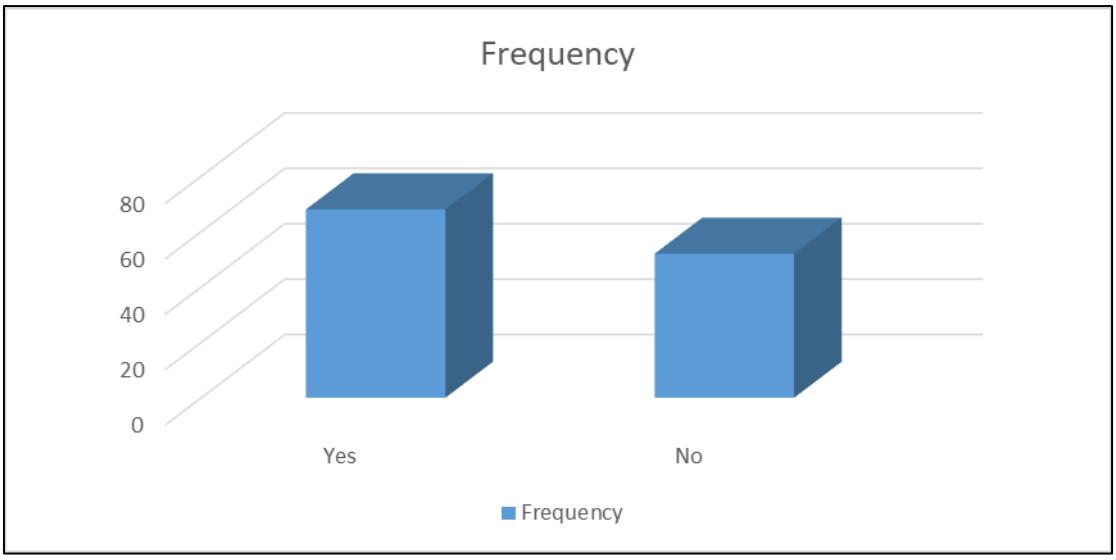

Figure 1 Formal inclusion of cyber hazards in SMS

A majority report cyber hazards are in the SMS registry, yet 43.3% still manage cyber risks outside SMS. This gap indicates missed opportunities for unified risk assessment and assurance (cf. Dave et al., 2022).

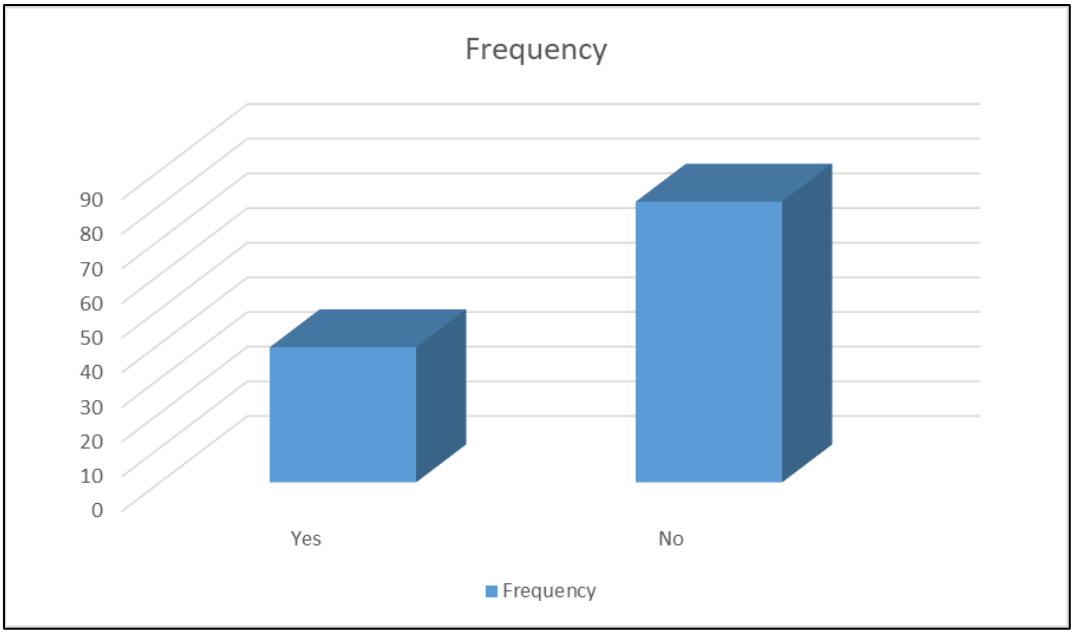

Figure 2 Cyber incident affecting operations in past 12 months

About a third experienced an operationally relevant cyber incident (e.g., ransomware on scheduling system, credential-phishing degrading dispatch). This aligns with literature noting active adversaries and aviation's expanding attack surface (Florido-Benítez, 2024).

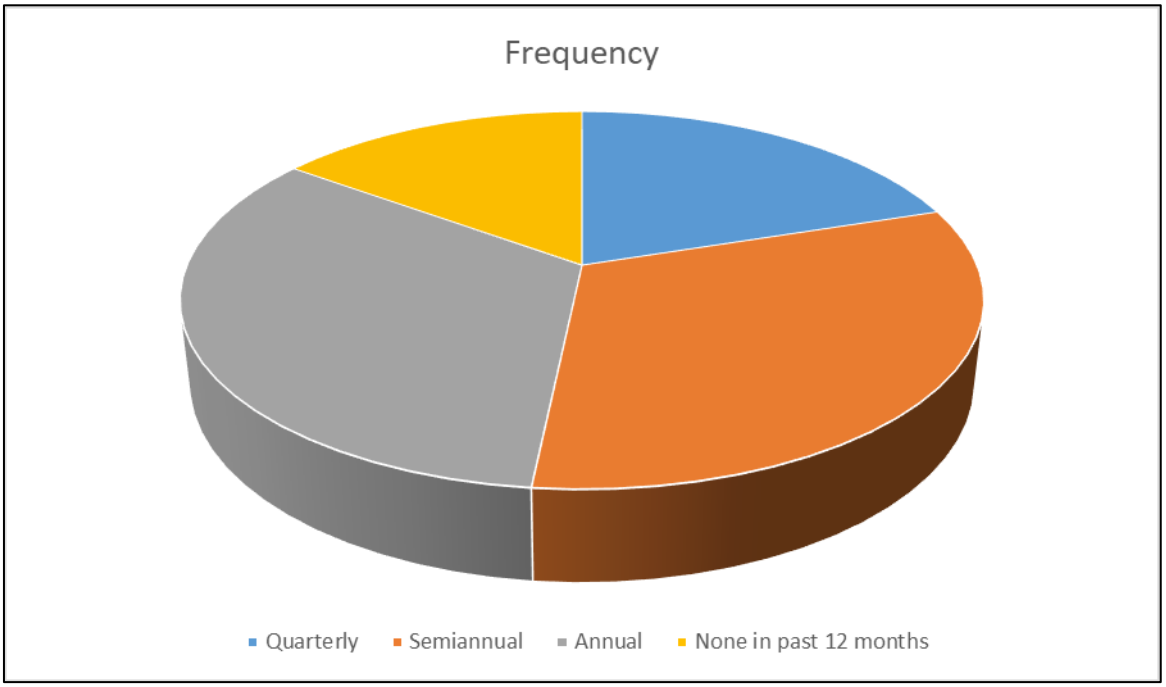

Figure 3 Training frequency on cyber-safety topics (flight/ops/maint.)

While most organizations provide at least annual training, 15% report none—an SMS promotion gap, given the human-factor vectors (phishing, weak EFB hygiene) highlighted in research (Lykou et al., 2019; Dave et al., 2022).

Table 2 Adoption of selected cyber controls

Control (Yes/No)	Yes (n)	Yes (%)	No (n)	No (%)
Multi-factor auth. for privileged & remote access	86	71.7	34	28.3
EFB hardening/baseline (MDM, app allow-listing, encryption)	78	65.0	42	35.0
SOC/SIEM monitoring for critical systems	49	40.8	71	59.2
Supplier/third-party cyber due-diligence for FBO/IT vendors	55	45.8	65	54.2

Foundational controls (MFA, EFB baselines) show higher adoption, but monitoring and supplier assurance lag. Given the literature on smart-airport interfaces and supply-chain risks, these shortfalls represent material residual risk that SMS should capture and treat (Lykou et al., 2019; Marisa & Coetzee, 2024).

5. Discussion

Findings reveal only partial alignment of cybersecurity efforts within Safety Management Systems (SMS). Although a substantial segment of operators acknowledges cyber threats, integration remains superficial; risks are neither documented nor managed in a consistent, systemic manner across all SMS stages. Our data, consistent with prior studies of Communication, Navigation, and Surveillance (CNS) vulnerabilities and adversary behavior (Dave et al., 2022; Florido-Benítez, 2024), report a 32.5% incident frequency, highlighting persistent operational exposure in business aviation—a realm characterized by small, multifunctional crews who balance aviation and cyber risk. Deficiencies identified in training and assurance (see Tables 1 and 2) indicate that the "Promotion" and "Assurance" components warrant immediate focus: deliver focused, scenario-driven cybersecurity training (phishing simulations for Electronic Flight Bag (EFB) users, strict protocols for secure software updates) and implement persistent oversight via Security Operations Centers (SOC) and Security Information and Event Management (SIEM) tools to limit attackers' dwell times and the potential for data exfiltration.

From a systems design standpoint, embedding cybersecurity within the SMS architecture carries three principal benefits. First, hazard identification is streamlined; once cyber risks such as the fabrication of performance data or the clandestine alteration of Minimum Equipment List (MEL) and Configuration Deviation List (CDL) documentation are recognised, they are integrated into the same bow-tie risk-analysis framework and the same risk register maintained for classic operational hazards (Chairopoulou, 2024). Unified management ensures that cyber vulnerabilities no longer exist as a parallel, disjoint inventory, reducing the chance of oversight and facilitating coordinated mitigation actions.

Common assurance loop. Cyber incidents undergo the same thorough investigation as traditional safety occurrences. Corrective and preventive actions are then recorded and tracked via the same safety action logs. Promotion and culture. Safety culture evolves to encompass a "cyber-safety culture" that institutionalizes secure behaviors: practicing password hygiene, handling electronic flight bags securely, and promptly reporting near-misses. Data-driven decision-making. Signals from monitoring alerts, phishing test scores, and patch latencies now serve as safety performance indicators, allowing management reviews to link cybersecurity and safety stewardship. These initiatives parallel ongoing guidance for aviation-specific security operations centers and-tiered risk frameworks

6. Conclusion

Cybersecurity more than ever influences business aviation safety (Ukwandu, et. al., 2022). Analysis in the literature repeatedly correlates cyber risk to safety performance across communications, navigation, surveillance systems, electronic flight bags, maintenance systems, and airport/operator hand-offs (Dave et al., 2022; Lykou et al., 2019; Florido-Benítez, 2024). Our survey confirms that more than half of operators presently incorporate cyber hazard assessment within the safety management system, yet monitoring, supplier assurance, and update frequency of staff training remain appreciable weaknesses. Adopting a cybersecurity-extended safety management system offers a practical, immediate means of addressing these vulnerabilities and strengthening operational firmness.

Recommendations

- Integrate cyber risks into SMS by cataloging cyber hazards in the existing SMS risk register; ensure hazard identification, risk control stages, and change management in SMS incorporate cyber scenarios in every safety risk assessment cycle.

- Provide continuous assurance by either establishing or outsourcing a Security Operations Center/Security Information and Event Management (SOC/SIEM) capability covering flight operations, operations control center, and aircraft maintenance systems; stipulate cyber-specific safety performance indicators, such as mean time to detect and mean time to respond.
- Fortify Electronic Flight Bag (EFB) security by mandating mobile device management that encrypts data at rest and transit, enforcing allow-lists for applications, distributing performance data through secure channels, and defining and rehearsing documented offline and emergency fallback procedures.
- Extend assurance to external providers by stipulating that fixed-base operators, information technology vendors, and data service companies submit cyber risk assessments and adopt contractual cybersecurity controls, vetted by same SMS oversight that governs internal systems.
- Cultivate a cyber-aware culture by providing role-based, hands-on cyber security training for aircrew, maintenance staff, and operational control center personnel at a minimum frequency of every six months, including phishing simulations within the workflow of the Electronic Flight Bag; document and report completion metrics as part of SMS performance indicators.
- Encourage thorough and barrier-free learning by classifying all cybersecurity incidents or near-misses as safety reportable occurrences; perform discipline-specific root cause analysis, cross-functional risk mitigations, and disseminate anonymized corrective actions organization-wide.
- Validate preparedness through cyber-specific emergency exercises simulating the loss of the operational scheduling system or the presence of a corrupted navigation database, to assess the effectiveness of contingency procedures and the robustness of inter-department communication protocols.

Compliance with ethical standards

Statement of informed consent

Informed consent was obtained from all individual participants included in the study.

References

[1] Marisa W. & Coetzee, M. (2024). Strengthening aviation cybersecurity with Security Operations Centres (SOC) for Air Traffic Management. Proceedings of the 19th International Conference on Cyber Warfare and Security. (Peer-reviewed conference paper discussing SOC frameworks for aviation/ATM).

[2] Chairopoulou, S. (2024). Cybersecurity in industrial control systems: a roadmap for fortifying operations (Master's thesis, Πανεπιστήμιο Πειραιώς).

[3] Dave, G., Choudhary, G., Sihag, V., You, I., & Choo, K. K. R. (2022). Cyber security challenges in aviation communication, navigation, and surveillance. Computers & Security, 112, 102516.

[4] Florido-Benítez, L. (2024). The types of hackers and cyberattacks in the aviation industry. Journal of Transportation Security.

[5] Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., & Janicke, H. (2020). A holistic review of cybersecurity and reliability perspectives in smart airports. IEEE Access, 8, 209802-209834.

[6] Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2019). Smart airport cybersecurity: Threat mitigation and cyber-resilience controls. Sensors, 19(1), 19.

[7] 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.