Law, Economics and Society; Vol. 1, No. 2; 2025
ISSN 3066-9340 E-ISSN 3066-9359
https://doi.org/10.30560/les.v1n2p1

Digital Saboteurs: Unmasking Insider Cybersecurity Threats in Aviation and Aerospace

Sharon L. Burton[1]

[1] College of Aviation, Embry-Riddle Aeronautical University, Daytona Beach, FL, United States.

Correspondence: Sharon L. Burton, College of Aviation, Embry-Riddle Aeronautical University, United States. Tel: 1-302-547-8010. E-mail: Burtons6@erau.edu

Received: May 22, 2025 Accepted: June 30, 2025 Online Published: July 15, 2025

Abstract

Insider risks in aviation and aerospace are frequently underestimated, perceived as isolated technical glitches rather than intentional acts capable of crippling air traffic control and endangering passengers. Comparable to arsonists who wield fire to destroy, these internal adversaries leverage their trusted positions to inflict financial loss, disrupt operations, and undermine organizational cohesion. The financial impact is significant, with incidents contained within a month averaging $10.6 million, while prolonged breaches can exceed $18 million. Such events consistently divert cybersecurity resources from strategic initiatives to reactive crisis management, imposing substantial ongoing costs on aviation organizations. This commentary-style article reframes insider cybersecurity threats using the metaphor of organizational arsonists, offering a unique and powerful framework for comprehending these complex risks in the aviation sector. This research adopts a multidisciplinary perspective, blending cybersecurity, legal frameworks, and psychological analysis to offer an extensive strategy for countering insider threats beyond purely technical solutions. It emphasizes the necessity of human-centric strategies, ethical accountability, and legal compliance, calling for aviation organizations to adopt a holistic defense posture that addresses technological vulnerabilities and behavioral risks. The article's originality lies in bridging multiple disciplines and framing insider threats as technical challenges and full-scale organizational crises within the aviation and aerospace industries. Combining advanced technologies such as artificial intelligence with human behavior analysis provides actionable strategies for aviation organizations to combat their digital arsonists. This interdisciplinary approach encourages cybersecurity professionals, legal scholars, and organizational leaders in aviation to rethink insider threat management, creating a more resilient and secure organizational environment.

Keywords: aviation cybersecurity, aviation administration, cybersecurity risk management, insider cybersecurity threats, insider threat detection, organizational arsonists, organizational behavior, organizational culture

1. Introduction

1.1 Introduction

The aviation and aerospace industries are confronted with substantial cybersecurity threats that can effect safety and national security. Recent incidents, for example, the Boeing data breach in 2023 (Baran, 2025; PetKauhas, 2023) and the Seattle-Tacoma Airport ransomware attack in 2024 (Lambert, 2024), highlight these risks. The financial burden of insider threats continues to be extensive, with average incident costs ranging from $10.6 million for events contained within a month to $18.7 million for longer breaches (Ponemon Institute & DTEX, 2025). These costs have risen 5% since 2024 and include investigation, prevention, and remediation expenses (Ponemon-Sullivan Report, 2023). Recent sector-wide analyses show that insider-related activities, including both malicious acts and negligent errors—constitute approximately 60% of all data breach incidents in aviation, with 55% of data loss events attributed to employee inattention (Majzoub, 2025). Globally, cyberattacks targeting aviation rose by 131% between 2022 and 2023, further intensifying the sector's risk profile (Davies, 2025). For example, in 2022, Pegasus Airlines experienced a major data exposure when a system administrator misconfigured cloud storage, leaving 6.5 terabytes of sensitive flight and crew data unprotected and highlighting the real-world impact of insider error (Syteca, 2025).

The financial impact of insider threats in aviation is substantial, with costs averaging $15 million per incident, not including potential losses from regulatory fines or litigation related to compromised safety (Mimecast, 2024). Sector-wide research indicates that insider-driven incidents now account for roughly 60% of all data breaches in aviation, with over half resulting from employee inattention or error (Majzoub, 2025). Globally, cyberattacks

targeting the aviation sector increased by 131% between 2022 and 2023, highlighting the urgency of addressing both technical and human vulnerabilities (Davies, 2025). Real-world cases, such as the 2022 Pegasus Airlines breach, where a misconfigured cloud storage bucket exposed 6.5 terabytes of sensitive data, demonstrate how a single insider mistake can have far-reaching operational and regulatory consequences (Syteca, 2025). These trends underscore the need for aviation organizations to adopt integrated, data-driven strategies to anticipate, detect, and mitigate insider threats.

The aviation sector's critical infrastructure status and its reliance on interconnected digital systems make it an attractive target for malicious actors (Lykou et al., 2018). Insider cybersecurity threats pose a particularly complex challenge for aviation organizations due to the sensitive and highly valuable data they manage, including flight plans, passenger information, and proprietary technological innovations (Lekota & Coetzee, 2019).

Unlike external threats, insider threats are especially pernicious because they originate from individuals who possess legitimate access to internal systems and databases, making detection and mitigation more challenging (Georgiadou et al., 2021). As given by Smith (2024), insider threats in aviation manifest in various forms, causing operational disruptions, compromising safety protocols, and damaging the organization's reputation. A nuanced understanding of insider threats in aviation requires recognizing that they can generally be categorized into malicious insiders, negligent insiders, and compromised insiders (Gheyas & Abdallah, 2016).

Insider threats in aviation can be broadly classified into three categories: malicious, negligent, and compromised insiders (Gheyas & Abdallah, 2016). These three categories are summarized in Figure 1. Malicious insiders are employees who deliberately misuse their authorized access to benefit themselves or to harm the organization, such as by leaking confidential data, sabotaging systems, or retaliating for perceived wrongs (Said, 2024). Their actions are intentional and often carefully orchestrated, posing direct risks to both organizational trust and aviation safety (Said, 2024).

Negligent insiders present a different but equally serious risk. These individuals, often unaware of the potential consequences, may inadvertently expose sensitive information or weaken security by falling for phishing attempts, mishandling confidential files, or misconfiguring critical systems (Cybersecurity & Infrastructure Security Agency, n.d.). Their mistakes, while unintentional, can still lead to significant breaches and operational disruptions.

Compromised insiders are employees whose credentials have been stolen by external attackers. Once in possession of legitimate access, these adversaries can bypass security controls, gaining entry to sensitive aviation systems under the appearance of authorized users (Klenka, 2021). Through methods such as social engineering and persistent cyberattacks, these intruders can move laterally within the network, targeting assets like air traffic control, maintenance records, or passenger data (Georgiadou et al., 2021). This scenario blurs the line between external and internal threats, creating a hazardous situation where the aviation industry’s most critical systems are vulnerable to exploitation by outsiders wielding insider-level access.

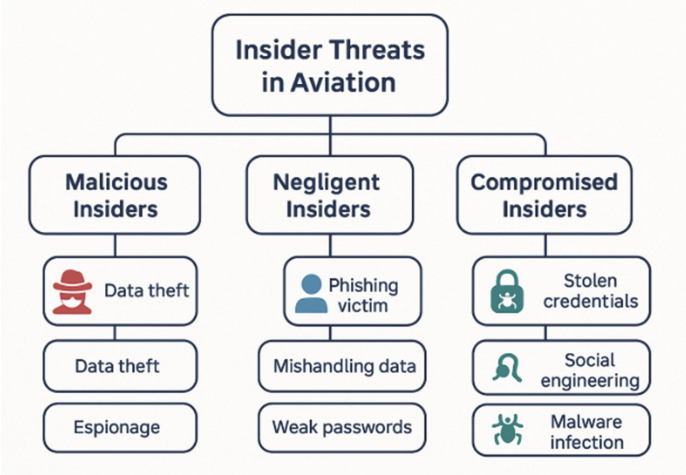

Figure 1. Insider Threat Categories in Aviation

Note. This figure illustrates the three primary categories of insider threats in aviation: malicious insiders (who intentionally cause harm), negligent insiders (who unintentionally create risk through carelessness or mistakes), and compromised insiders (whose credentials are misused by external actors). These categories are adapted from Gheyas & Abdallah (2016) and reflect the taxonomy applied throughout this study.

The aviation industry is confronting a surge in insider threat challenges, propelled by a convergence of technological and organizational factors. The introduction of electric vertical takeoff and landing aircraft, expanded use of drones, advancements in surveillance, and the integration of artificial intelligence have all increased the sector's operational complexity and digital exposure (Industrial Cyber, 2024). The exceptional value of aviation data, and the potentially devastating impact of its compromise, renders the sector especially attractive to both cybercriminals and state-sponsored actors, who frequently exploit insider access to bypass traditional defenses (Bovenizer, 2024; Eleimat & Őszi, 2025). These risks are further compounded by the intricate and interconnected nature of aviation IT infrastructure, where vulnerabilities in one area can rapidly propagate across the organization (Bovenizer, 2024). As the industry continues to adopt next-generation air traffic management, in-flight connectivity, and automated operations, the resulting technological ecosystem offers both enhanced efficiency and a broader attack surface, presenting persistent security challenges (Federal Aviation Administration [FAA], 2024).

Moreover, as given by Kizilcan and Mizrak (2022), the void of thorough cybersecurity training among aviation professionals exacerbates the problem. The data shows that there are employees whom are unprepared to recognize sophisticated cyber threats such as targeted phishing campaigns or social engineering tactics, making them prime targets for attackers who rely on human vulnerabilities. The high-pressure nature of aviation operations compounds the issue. Under immense stress and time constraints, employees may prioritize immediate operational needs over security protocols, often forgetting to log out of shared systems or mishandling sensitive information (Nobles, 2022).

1.2 Statement of the Problem

This scholarly commentary category article endeavors to reconceptualize insider cybersecurity threats in the aviation sector as deliberate disruptors (i.e., individuals who, akin to arsonists within digital landscapes, methodically ignite operational chaos to serve personal or ideological ends). Much like their real-world counterparts, these internal adversaries leverage their insider familiarity to pinpoint and exploit critical weaknesses in organizational systems with surgical accuracy (Jones, 2024). Their actions have sweeping concerns, prompting organizational confusion, receivership concerns, and severe legal consequences that can ripple through the entire aviation industry.

By invoking the metaphor of an internal saboteur, the article underscores the dual technical and behavioral facets of insider risk. This multidisciplinary approach, merging cybersecurity, legal, and psychological perspectives, advocates for strategies that extend beyond technology alone. Commentary articles are crucial in academic discourse because they provide a platform for thought leadership, challenge established paradigms, and propose innovative solutions. This article adheres to that tradition by synthesizing existing research and practical insights

into a cohesive narrative that advocates for strategic change in aviation cybersecurity practices. This work aims to stimulate dialogue among cybersecurity professionals, legal scholars, and aviation industry leaders, encouraging them to rethink how insider threats are perceived and addressed in this critical sector.

By foregrounding the complex interplay among behavioral dynamics, legal frameworks, and technological countermeasures, the article advocates for a sophisticated and integrated strategy to confront insider cybersecurity threats in the aviation sector. This approach is particularly crucial given the potential for insider threats to compromise not only organizational assets but also public safety and national security interests.

1.3 Methodology

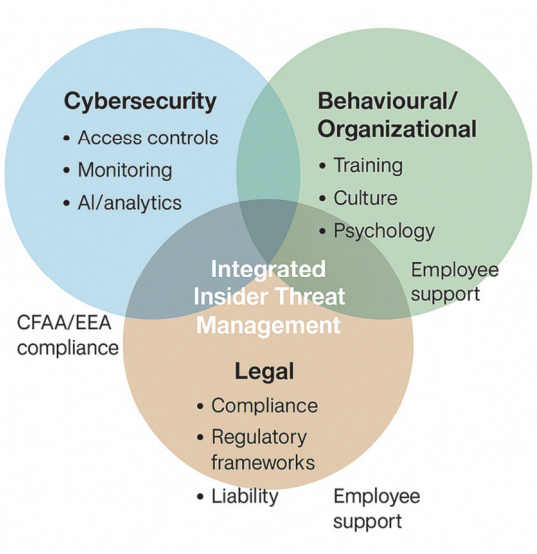

Figure 2. Multidisciplinary Framework for Insider Threat Management in Aviation

Note. This diagram illustrates the integrated approach used in this study, combining technical (cybersecurity), legal, and behavioral/organizational strategies to address insider threats in aviation. The framework emphasizes that effective mitigation requires collaboration across these domains, with each discipline contributing unique tools and perspectives to strengthen overall security and resilience.

The analysis synthesizes insights from technical, legal, and behavioral disciplines, integrating recent research and industry case studies to reflect the latest developments and best practices in aviation security. The multidisciplinary framework guiding this analysis is illustrated in Figure 2, which demonstrates how technical, legal, and behavioral strategies are integrated to address insider threats in aviation. The selection of sources prioritizes recent developments and authoritative voices within the field, ensuring that the discussion reflects current challenges and best practices. Each cited work is evaluated for its applicability to the aviation context, with particular attention to the intersection of technological vulnerabilities, human factors, and regulatory environments. By integrating technical, legal, and behavioral strategies, and by fostering a culture of vigilance and accountability, aviation and aerospace organizations can safeguard their critical assets, protect public safety, and uphold their commitment to operational excellence in the face of evolving insider threats.

1.4 Significance of the Problem

Empirical instances underscore the profound implications of insider threats within the aviation sector, demonstrating their severity and extensive ramifications. Notably, personnel entrusted with elevated access privileges may intentionally divulge critical operational intelligence to external adversaries, thereby undermining flight safety frameworks and exposing latent weaknesses in airport security infrastructures. Conversely, inadvertent lapses by aviation staff (i.e., the erroneous transmission of confidential flight documentation or passenger records to unauthorized parties) can precipitate the exposure of sensitive data and contravene global data protection mandates (Kizilcan & Mizrak, 2022; Jones, 2024).

The proliferation of ransomware attacks instigated by phishing campaigns directed at aviation personnel is a matter of pressing concern. Under such circumstances, an employee lacking sufficient awareness may activate a malicious hyperlink, unwittingly facilitating the infiltration of ransomware into the organization's digital infrastructure.

These breaches can incapacitate comprehensive aviation networks, resulting in operational paralysis and the compromise of mission-critical functionalities, including air traffic management and maintenance coordination (Georgiadou et al., 2021).

Similarly, the illicit dimension of insider threats is frequently rooted in the deliberate exploitation of privileged system access, manifesting in behaviors such as the misappropriation of intellectual property, fraudulent activities, operational sabotage, and acts of espionage. These actions not only undermine the integrity of aviation operations but also expose organizations to substantial legal and regulatory risks (Leppard Law Firm, 2024; National Counterintelligence and Security Center [NCSC], 2025). Insider threats may result in severe legal and regulatory consequences for aviation organizations.

The proliferation of ransomware attacks instigated by phishing campaigns directed at aviation personnel is a matter of pressing concern. Under such circumstances, an employee lacking sufficient awareness may activate a malicious hyperlink, unwittingly facilitating the infiltration of ransomware into the organization's digital infrastructure. These breaches can incapacitate comprehensive aviation networks, resulting in operational paralysis and the compromise of mission-critical functionalities, including air traffic management and maintenance coordination (Georgiadou et al., 2021).

The illicit dimension of insider threats in aviation often stems from the deliberate misuse of privileged access, resulting in actions such as intellectual property theft, fraud, operational sabotage, and espionage. These behaviors undermine the integrity of aviation operations and expose organizations to significant legal and regulatory risks (Leppard Law Firm, 2024; National Counterintelligence and Security Center [NCSC], 2025). Insider threats may result in severe legal and regulatory consequences for aviation organizations.

Beyond the purview of criminal sanctions, aviation organizations face substantial legal exposure in civil, employment, and regulatory domains when responding to insider threats (Klenka, 2021). The indeterminate nature of intent in such incidents presents considerable legal complexity, often necessitating detailed forensic inquiry and specialized legal analysis to discern criminal culpability from inadvertent error within the high-consequence context of aviation (Gelles, 2021). Regulatory frameworks must remain adaptive, continuously addressing the evolving tactics of insider threats while ensuring that legal responses harmonize security imperatives with the protection of employee rights and the cultivation of a vigilant, accountable organizational culture.

The legal risks associated with insider threats in aviation are both extensive and complex. Deliberate acts such as fraud, sabotage, or espionage can expose individuals and organizations to serious criminal, civil, and regulatory consequences, especially when these actions threaten public safety or disrupt critical operations (National Insider Threat Special Interest Group [NITSIG], 2021). Aviation organizations must be prepared to navigate these intricate legal challenges, as insider threats may result in severe penalties and long-term reputational harm (United States Department of Justice, 2021; Burrell et al., 2023).

Employment law intersects critically with cybersecurity in the context of insider threat management. While termination for cause is a typical organizational response to insider misconduct, aviation entities must exercise caution to avoid litigation for wrongful termination, particularly given the specialized expertise required in many industry roles. In instances of negligence, liability may accrue to the individual and the organization, potentially resulting in regulatory penalties if insufficient cybersecurity measures contribute to data breaches or safety incidents (Leppard Law Firm, 2021).

Addressing insider risk requires a comprehensive strategy that balances technological solutions with initiatives focused on human behavior and organizational culture. Organizations must establish robust internal controls while preserving the delicate balance between security imperatives and employee trust, an especially sensitive dynamic in an industry where safety and operational efficiency are paramount (Burrell et al., 2023). As aviation and aerospace organizations navigate this challenge, the following section explores how integrating behavioral analytics and advanced monitoring technologies can strengthen defenses against insider threats while supporting a culture of accountability and vigilance.

The task of monitoring employee conduct without infringing upon privacy rights is further complicated by the international scope of many aviation operations and the variability of privacy legislation across jurisdictions. Achieving an appropriate equilibrium between proactive surveillance and respect for employee privacy requires judicious consideration of legal and ethical dimensions specific to the aviation sector. This complexity is heightened by the diversity of insider threat profiles, ranging from malicious actors with extensive system knowledge to well-intentioned but negligent employees who may inadvertently undermine security (Georgiadou et al., 2021).

Psychological stressors (i.e., dissatisfaction, financial hardship, and operational pressure) significantly increase the likelihood of insider incidents. Addressing these underlying issues is essential for reducing risk. Organizations that neglect to address these underlying issues risk fostering an environment conducive to insider threats, particularly among personnel with access to critical systems or sensitive information (Nobles, 2022).

Intentional and illicit insider-driven data loss in aviation can be likened to digital arson, deliberate acts of sabotage that deplete financial resources, disrupt core operations, and erode the resilience of cybersecurity teams entrusted with safeguarding vital infrastructure. Analogous to an arsonist who targets physical assets, insider adversaries exploit their privileged access to incite chaos within digital systems that govern everything from flight operations to passenger safety (Jones, 2024).

The financial impact of insider threats in aviation is substantial, with costs averaging $15 million per incident, not including potential losses from regulatory fines or litigation related to compromised safety (Mimecast, 2024). Sector-wide research indicates that insider-driven incidents now account for roughly 60% of all data breaches in aviation, with over half resulting from employee inattention or error (Majzoub, 2025). Globally, cyberattacks targeting the aviation sector increased by 131% between 2022 and 2023, highlighting the urgency of addressing both technical and human vulnerabilities (Davies, 2025). Real-world cases, such as the 2022 Pegasus Airlines breach, where a misconfigured cloud storage bucket exposed 6.5 terabytes of sensitive data, demonstrate how a single insider mistake can have far-reaching operational and regulatory consequences (Syteca, 2025). These trends underscore the need for aviation organizations to adopt integrated, data-driven strategies to anticipate, detect, and mitigate insider threats.

On May 6, 2022, the Threathunt 2030 conference convened prominent cybersecurity stakeholders from EU Member States, alongside representatives from European Union institutions and agencies, to collaboratively explore the detection and assessment of nascent and evolving cybersecurity threats. The primary objective of the event was to deliberate on contemporary tools, resources, and analytical methodologies that could be leveraged to anticipate potential threats likely to materialize by 2030, thereby ensuring that the European cybersecurity infrastructure remains sufficiently prepared to address such challenges with agility and efficacy (Garcia-Blanco, 2022). The European Union Aviation Safety Agency (EASA) contributed as a participant in the panel dedicated to sector-specific cybersecurity challenges.

This sector-focused panel assembled experts from the railway, aviation, maritime, and energy industries to examine the ongoing transition from analog to digital technologies, as well as the increasing interconnectedness among these sectors. The discussion highlighted how advancements such as drone integration, remote control capabilities, augmented reality in aviation cockpits, GPS interference, and the deployment of artificial intelligence in cyber-attacks are collectively broadening the scope of potential vulnerabilities. In this context, the imperative for robust information sharing and collaborative threat intelligence among industry stakeholders was underscored (Garcia-Blanco, 2022).

Cybersecurity executives operating within the aviation sector encounter profound psychological demands, reminiscent of orchestrating responses to an ongoing series of unforeseen crises within a high-stakes environment where safeguarding public welfare is of utmost priority. This challenge is further intensified by the accelerating digital transformation and the proliferation of interconnected devices, with a growing proportion of critical services and communications now relying on wireless technologies (Dave et al., 2022).

Results from the 2024 Data Exposure Report denote that 72% of cybersecurity leaders fear job loss if an insider breach goes unanswered (GlobeNewswire, 2024). The intersection of employee age and organizational function introduces deeply unsettling vulnerabilities to data security, amplifying anxieties among corporate leaders about insider risks.

Further, the 2024 Data Exposure Report highlights a disquieting trend. Organizations are increasingly alarmed by the heightened susceptibility of Generation Z and Millennial employees to security incidents, with substantial percentages falling prey to (61%) phishing attacks, (60%) carelessly disseminating proprietary information online, (62%) transferring corporate files to personal devices, and (58%) inappropriately inputting sensitive data into generative AI platforms (GlobeNewswire, 2024). Additionally, survey participants further identified senior executives (81%) and board members (71%) as presenting the most significant risk to organizational data security, a perception likely stemming from their extensive access to highly confidential information (GlobeNewswire, 2024). This confluence of generational and role-specific vulnerabilities engenders considerable apprehension among security teams as they contend with an increasingly fluid and unpredictable threat landscape.

Imagine a scenario in which a highly trusted employee, exploiting their authorized system privileges, deliberately transfers confidential information regarding aircraft vulnerabilities to a foreign actor. Such incidents transcend the

realm of technical vulnerabilities, escalating into profound organizational crises characterized by reputational harm, legal and regulatory repercussions, significant shifts in internal culture, and sustained competitive disadvantages. The ramifications of these breaches endure well beyond immediate financial losses and operational disruptions, shaping the organization's trajectory for years to come (United States Government Accountability Office, 2020; Gimarelli, 2025). The intersection of fiscal, functional, and emotional stressors highlights the imperative for forward-thinking, comprehensive approaches to combat insider threats within the aviation sector. Effective solutions must harmonize advanced technical safeguards with nuanced insights into individual conduct and the distinctive cultural dynamics of aviation organizations, environments in which the consequences of security lapses are especially severe.

1.5 Assumptions, Limitations, and Delimitations

This commentary proceeds under several foundational assumptions that shape its analysis and recommendations. First, it assumes that insider threats in aviation and aerospace are best understood through a multidisciplinary lens, integrating technical, behavioral, and organizational perspectives. Second, it presumes that the metaphor of the organizational arsonist provides a valuable and accurate framework for conceptualizing intentional insider threats, enabling stakeholders to grasp the severity and complexity of these risks. Third, it assumes that aviation and aerospace organizations have the capacity and willingness to invest in advanced monitoring technologies and robust security cultures despite financial and operational constraints. Finally, it operates on the premise that effective insider threat mitigation requires ongoing adaptation and collaboration among industry leaders, regulators, and cybersecurity professionals.

This analysis is subject to several significant limitations. First, the selection of case studies may introduce bias, as cases are often chosen based on their availability, prominence, or the level of detail provided in public records. Such a selection process can inadvertently emphasize high-profile incidents while overlooking less-publicized but equally relevant events, potentially limiting the generalizability of the findings. Additionally, the reliance on documented cases may underrepresent insider threats that remain undetected or unreported, further shaping the narrative toward more visible breaches.

Second, while the discussion highlights the promise of advanced monitoring technologies (i.e., AI-driven User and Entity Behavior Analytics) for detecting insider threats, it is significant to recognize that the adoption of these solutions is not uniform across the aviation sector. Many organizations, particularly those with limited financial or technical resources, may face significant barriers to implementing and maintaining sophisticated monitoring systems. The high costs associated with acquiring, integrating, and operating AI-based tools can restrict their use to larger or better-funded entities, leaving smaller organizations more vulnerable to insider risks.

Finally, this article draws on a combination of industry reports, peer-reviewed literature, and selected case studies to inform its analysis. While this approach provides a broad perspective, it may not capture the full diversity of organizational experiences or account for evolving threat landscapes. Future research should aim to incorporate a broader range of case examples and explore alternative monitoring strategies that are accessible to organizations with varying resource levels.

This commentary intentionally narrows its scope to address specific aspects of insider cybersecurity threats. First, it concentrates on the aviation and aerospace sectors, recognizing their unique operational and regulatory environments as distinct from other critical infrastructure domains. Second, it emphasizes intentional insider threats, those driven by malice, revenge, or personal gain, while acknowledging but not extensively analyzing accidental or negligent insider actions. Third, the analysis prioritizes recent developments and best practices, focusing on the period from 2020 to 2025 to ensure relevance to current challenges. Finally, the commentary does not provide a comprehensive review of all potential technical solutions or legal frameworks but instead highlights those most pertinent to the multidisciplinary, human-centric approach advocated by Dr. Burton.

1.6 The Ingenuity of the Organizational Arsonist Metaphor in Aviation Cybersecurity

The distinctive contribution of this article emerges from its innovative portrayal of insider cybersecurity threats as agents of digital sabotage within the aviation sector. This conceptual leap fundamentally reshapes how insider risk is understood in relation to broader aviation security imperatives. While conventional analysis tends to compartmentalize such threats as mere technical malfunctions or discrete data breaches, this article underscores their capacity to ripple through every layer of organizational and operational integrity. By transcending narrow interpretations, it sets the stage for a more nuanced appreciation of how insider actions can undermine not just information systems but the very fabric of aviation safety and national security.

Rather than viewing insider threats as isolated events, this article elucidates their potential to erode organizational cohesion, diminish workforce confidence, and disrupt critical functions in ways that are uniquely perilous for the aviation industry. The metaphor of digital arson is employed to vividly illustrate how malicious insiders can ignite crises that spread rapidly through interconnected systems, threatening far more than individual data points. This perspective enables stakeholders to grasp the profound and cascading consequences that insider-driven security failures can precipitate in environments where operational continuity is paramount.

A hallmark of this article's approach is its synthesis of insights from multiple domains, including technical cybersecurity, legal accountability, behavioral psychology, and organizational studies, all viewed through the lens of aviation's distinctive operational landscape. It champions the integration of advanced technologies such as artificial intelligence and behavioral analytics with strategies that address the human dimensions of risk, thereby offering a robust and adaptive response to insider threats. This interdisciplinary orientation marks a significant evolution beyond conventional, technology-centric security paradigms.

By harmonizing the analysis of human motivations and vulnerabilities with the deployment of cutting-edge security technologies, the article delivers a comprehensive framework for understanding and mitigating insider threats in aviation. It not only reimagines the narrative around insider risk but also furnishes practical guidance for organizations seeking to fortify their defenses against intentional and inadvertent internal threats. The result is a proactive, context-sensitive model that acknowledges the psychological, ethical, and technological complexities inherent in safeguarding aviation infrastructure.

This reconceptualization is especially pertinent given the aviation sector's global interconnectivity and the vital significance of its infrastructure to economic and national security. The article's holistic framework provides actionable strategies for enhancing organizational resilience and preparedness in the face of evolving threats. Ultimately, it makes a significant contribution to the advancement of aviation cybersecurity by offering insights that are theoretically robust and practically relevant for industry stakeholders.

1.7 The Progression and Intricacy of Insider Threats in Aviation

The emergence of insider threats as a significant risk within the aviation sector became particularly apparent during the 1990s, as organizations increasingly adopted advanced information technology systems, such as digital flight planning, maintenance tracking, and cargo logistics (Weber, 2025). These technological advancements granted employees access to sensitive systems and data at unprecedented levels, fundamentally altering the security landscape. Historically, insider threats in aviation, dating back to the 1970s, have involved individuals attempting to carry out malicious intent through physical means rather than through cyber-enabled methods (Krull, 2016). The spectrum of insider threats spans from low-level employees, such as baggage handlers and IT workers, to high-level managers and officers. This breadth highlights persistent gaps in security measures related to access controls and the assignment of privileges based on legitimate operational needs (Krull, 2016).

Initially, insider threats in aviation appeared manageable, as most organizational networks were self-contained and isolated from external connections. However, the rapid expansion of internet connectivity and the integration of digital technologies into every aspect of aviation operations in the early 2000s shattered these boundaries, exponentially increasing the pathways through which individuals with privileged access could engage in destructive behavior. A security paradox arose, creating a dilemma: operational efficiency required broad employee access, but this very access introduced new vulnerabilities, especially when misused intentionally or negligently. The challenge for aviation organizations became clear as they sought to balance the need for productivity with the imperative to protect critical assets (Davies, 2025).

The potential for internal threats grew alongside technological advances, transforming insider risk into a dynamic and complex issue that permeates all levels of aviation operations, from ground services to in-flight systems. The interconnectedness of modern aviation systems, including air traffic control, passenger processing, and aircraft maintenance, has created a vast digital ecosystem where a single point of compromise can have far-reaching consequences. The aviation industry's unique characteristics further amplify the complexity of insider threats. Its critical role in national security and global commerce makes it an attractive target for malicious actors, external and internal. The vast amounts of sensitive data processed daily, from passenger information to flight plans and maintenance schedules, create numerous opportunities for exploitation. Moreover, the industry's reliance on a diverse workforce, including contractors and temporary staff, introduces additional vulnerabilities that malicious insiders can exploit.

As aviation technology continues to advance, with the integration of artificial intelligence, autonomous systems, and the Internet of Things, the attack surface for insider threats expands correspondingly. These technological

advancements, while enhancing operational efficiency and safety, also introduce new vulnerabilities that insiders with technical expertise can potentially exploit (Georgiadou et al., 2021).

1.8 Behavioral Analytics in Aviation

While initial efforts focused on strengthening technical defenses, organizations soon realized that effective risk management also requires monitoring behavioral patterns and enforcing strict access controls, such as the principle of least privilege (ICAO, 2022; Malik, 2025). The complexity of insider threats necessitated a broader perspective, one that considered not only the security of operational technology (OT) and Internet of Things (IoT) systems, which are integral to ensuring passenger safety but also the significance of comprehending human behavior and motivation (Malik, 2025; Nobles, 2022). This shift underscored the imperative of integrating behavioral insights and psychological analysis into cybersecurity strategies, thereby enabling organizations to more effectively anticipate, detect, and mitigate risks posed by insiders.

As insider threats became more deeply entrenched within the aviation cybersecurity landscape, organizations recognized the necessity of evolving their strategies beyond traditional technical defenses (ICAO, 2022). Initial efforts concentrated on fortifying firewalls, implementing encryption protocols, and refining access control systems to prevent unauthorized entry. However, it soon became apparent that these measures alone were insufficient for mitigating the full spectrum of cybersecurity risks (Malik, 2025).

User and Entity Behavior Analytics, or UEBA, is a special computer program that watches how people and devices behave on a network. It learns what is normal and then looks for anything unusual or strange that might mean someone is doing something bad. In UEBA, “users” are people like employees who use computers, and “entities” are things like computers, servers, or devices that also use the network. The program watches both to keep everything safe. In response, the aviation sector began to adopt advanced monitoring technologies, such as User and Entity Behavior Analytics (UEBA), which continuously analyzes user activities to detect deviations that may indicate malicious intent. The effectiveness of these systems relies on the availability of accurate, comprehensive data, which is essential for the timely identification and prevention of cyber threats within aviation infrastructures. For instance, should an employee begin accessing sensitive flight data at unusual hours or download large volumes of passenger information without a legitimate business purpose, traditional security tools might overlook these anomalies. However, behavior-based analytics can flag such activities as potential indicators of insider threats (Nobles, 2022). This shift underscores the significance of integrating technological safeguards and a nuanced understanding of human behavior and motivation, as operational technology and IoT systems are vital to passenger safety and require vigilant oversight (Malik, 2025; Nobles, 2022). By combining real-time anomaly detection with robust access management and a focus on behavioral risk factors, aviation organizations can more effectively anticipate, detect, and mitigate insider threats, thereby enhancing the overall resilience of critical aviation systems.

Consider, for example, an employee who initiates access to sensitive flight data during irregular hours or downloads substantial volumes of passenger information without a justifiable operational need. While standard security protocols may fail to recognize such deviations, behavior-based analytics are capable of detecting these irregularities and alerting security teams to potential insider threats (Nobles, 2022). This integration of sophisticated analytics with rigorous data standards represents a critical advancement in safeguarding aviation systems against the evolving risks posed by insiders.

The adoption of the principle of least privilege, which limits employee access strictly to the data and systems required for their specific duties (Plachkinova & Knapp, (2023), has become a fundamental element in mitigating insider threats within the aviation sector. By minimizing the scope of available privileges, organizations effectively reduce the potential attack surface that malicious insiders could exploit while also significantly lowering the risk of inadvertent data exposure by well-intentioned staff (ICAO, 2022; Ponemon Institute & DTEX, 2025). This strategy is especially vital in aviation, where unauthorized access to critical operational or safety systems could result in immediate and far-reaching consequences for organizational integrity and public security (Federal Aviation Administration [FAA], 2024). The principle of least privilege not only supports robust cybersecurity postures but also aligns with regulatory compliance and industry best practices for access control and risk management in high-stakes environments.

1.9 Navigating the Human Element: Aviation Cybersecurity Leadership in the Era of Insider Threats

The responsibilities of cybersecurity leaders within the aviation sector have undergone a notable transformation as the landscape of insider threats has grown more intricate and pervasive (Ukwandu et al., 2022). As given by Effective knowledge management is essential in aviation cybersecurity to capture, share, and retain critical information. It supports continuous learning, enhances organizational resilience, and ensures that employees are well-prepared to address evolving insider threats. Integrating knowledge management practices with cybersecurity

strategies fosters a culture of informed vigilance and adaptive response (Reddy Dodla, 2024). In this environment, effective leadership extends well beyond technical proficiency, necessitating a comprehensive approach that integrates advanced technological knowledge with a nuanced understanding of psychological and behavioral dynamics, as well as the unique cultural aspects of aviation organizations (Nobles, 2019; 2022). Contemporary leaders must actively interpret subtle shifts in employee conduct, recognize motivational undercurrents, and anticipate risks that could precipitate insider incidents specific to the operational realities of aviation.

Comprehending and aligning with employee motivations is essential for the early detection and mitigation of insider risks. While financial incentives or ideological objectives typically drive external attackers, insiders within aviation organizations are more likely to be influenced by personal grievances, professional dissatisfaction, or a sense of injustice (ICAO, 2022; Jones, 2024). Leaders who fail to address these underlying factors may inadvertently allow latent threats to escalate, resulting in security breaches that could have been preempted through timely and empathetic intervention. For instance, an air traffic controller who feels overlooked for advancement may demonstrate signs of disengagement, such as withdrawing from collaborative efforts and declining productivity, ultimately heightening their susceptibility to actions that undermine organizational integrity and aviation safety (National Academies of Sciences, Engineering, and Medicine, 2025). Proactive leadership, attuned to the technical and human dimensions of risk, is therefore indispensable for safeguarding critical aviation infrastructure against insider threats.

1.10 Workplace Deviant Behaviors

The concept of workplace deviance, while rooted in organizational and sociological research (Robinson & Bennett, 1995), has become increasingly pertinent to discussions of insider risk within the aviation sector. Workplace deviance encompasses a broad range of voluntary behaviors that contravene established organizational norms and jeopardize the well-being of the organization or its members (Robinson & Bennett, 1995). Within aviation, such behaviors can have especially severe ramifications, threatening not only operational integrity but also the safety and security of passengers, crews, and critical infrastructure (Robinson & Bennett, 1995). In this context, workplace deviance manifests across a spectrum, from unintentional errors to deliberate acts of sabotage, each presenting distinct challenges for cybersecurity and risk management.

Three primary categories of workplace deviance are particularly relevant to aviation cybersecurity: accidental, negligent, and malicious actions. Accidental deviance arises when employees, often due to insufficient training or awareness, inadvertently violate security protocols. For example, a well-meaning airline employee might unknowingly transmit confidential flight plan data to an unauthorized recipient or upload sensitive passenger manifests to an insecure cloud service. Though the intent is not malicious, the consequences can be severe, potentially resulting in data breaches, financial losses, and reputational harm (Nobles, 2022).

Negligent deviance involves employees who, despite being aware of established security protocols, consciously disregard them without malicious intent. This act might occur when an aircraft maintenance technician routinely bypasses password security requirements, mistakenly believing such measures are unnecessary. Such behaviors leave organizations vulnerable to cyber threats that could compromise critical systems and, ultimately, flight safety (Burrell et al., 2023).

The most severe form of workplace deviance is malicious deviance, which includes deliberate acts intended to harm the organization or its members. These actions may be motivated by personal grievances, a desire for revenge, financial gain, or even espionage. In aviation, malicious insiders might plant malware, leak sensitive data, or disrupt air traffic control systems, causing widespread operational disruption and endangering lives (Garg & Sharma, 2025).

Within the broader framework of workplace deviance, additional subcategories further elucidate the motivations and manifestations of insider threats. Workplace retaliation or revenge refers to actions taken by employees seeking retribution for perceived injustices (U. S. Equal Employment Opportunity Commission, (n.d), while workplace aggression describes harmful behaviors directed at colleagues or the organization itself (Quinn et al., 2025). Both forms can exacerbate existing vulnerabilities in aviation cybersecurity, particularly when combined with the sector's complex, interconnected digital infrastructure and high, stakes operational environment.

Comprehending and addressing workplace deviance requires a multifaceted approach that integrates technical safeguards with robust training, continuous monitoring, and a strong organizational culture that prioritizes security and accountability. By recognizing the full spectrum of deviant behaviors, from accidental missteps to deliberate sabotage, aviation organizations can better anticipate, detect, and mitigate insider threats, thereby safeguarding their assets and the broader public interest.

1.11 The Organizational Arsonist: Metaphor and Realities of Malicious Insider Threats in Aviation

Malicious deviance represents the most perilous form of workplace misconduct in the aviation sector, characterized by deliberate actions intended to harm the organization, its members, or its critical infrastructure (Robinson & Bennett, 1995). These behaviors, including sabotage, data exfiltration, and espionage, are often motivated by financial gain, personal vendettas, or ideological objectives and pose a significant threat to aviation safety, operational continuity, and national security (Gimarelli, 2025; Mahdi & Assim, 2025; Labree et al., 2010). Sabotage, as defined by Mahdi and Assim (2025), involves the intentional disruption or destruction of organizational operations, which in aviation can manifest as deletion of critical flight data, leaking of sensitive security information, or corruption of digital systems, each leaving a trail of chaos in its wake.

The emergence of the "organizational arsonist" metaphor in aviation cybersecurity underscores the parallels between physical arson and digital sabotage, highlighting the deliberate, calculated nature of these insider threats (Jones, 2024; Lauzier, 2025). Modern digital arsonists exploit their privileged access to ignite metaphorical fires within critical aviation systems, causing disruption that can ground fleets, compromise safety protocols, and endanger lives. Their actions are frequently planned and methodical, leveraging insider knowledge to bypass conventional defenses and maximize damage while evading detection (Said, 2024; Ukwandu et al., 2022).

The psychological motivations of digital arsonists often mirror those of traditional arsonists, ranging from anger and revenge to a desire for recognition or control (Labree et al., 2010; ICAO, 2022). In aviation, these individuals may target sensitive data, operational technology, or safety-critical infrastructure, exploiting the interconnectedness of modern aviation enterprises. The metaphor not only highlights the technical and behavioral complexity of insider threats but also unites diverse stakeholders, cybersecurity professionals, legal experts, and organizational leaders, around a shared understanding of risk (Jones, 2024).

Addressing malicious insider threats requires a comprehensive approach that integrates advanced technical safeguards, behavioral analytics, and a strong organizational culture of accountability and vigilance (ICAO, 2022; Malik, 2025). By framing insider risk through the lens of digital arson, aviation organizations can better appreciate the cascading and unpredictable nature of these threats, reinforcing the need for proactive prevention, early detection, and coordinated response.

1.12 Legal Implications of Insider Threats in Aviation

Insider threats in aviation not only disrupt operations and undermine safety but also carry significant legal consequences. U.S. federal statutes such as the Computer Fraud and Abuse Act (CFAA) and the Economic Espionage Act (EEA) are central to prosecuting individuals who intentionally misuse privileged access to harm aviation organizations (Leppard Law Firm, 2024; National Counterintelligence and Security Center [NCSC], 2025; United States Department of Justice, 2021). The CFAA criminalizes unauthorized access to protected computer systems, data exfiltration, and intentional disruption of critical operations, with heightened penalties when such acts affect critical infrastructure. The EEA addresses the theft or misappropriation of trade secrets, including the transfer of proprietary aviation technology or operational data to foreign entities, and imposes both criminal and civil penalties for economic espionage and commercial theft.

Beyond criminal prosecution, aviation organizations face exposure to civil, regulatory, and employment law actions when responding to insider incidents (Klenka, 2021). Determining whether an act was malicious or negligent often requires detailed forensic investigation and legal analysis, especially given the high-consequence environment of aviation (Gelles, 2021). Regulatory frameworks must remain adaptive, balancing proactive security measures with employee rights and privacy. Effective insider threat management, therefore, demands not only technical and behavioral controls but also a thorough understanding of the evolving legal landscape, ensuring compliance while protecting both organizational assets and individual rights (National Insider Threat Special Interest Group [NITSIG], 2021; Burrell et al., 2023).

Figure 3. Multidisciplinary Landscape of Insider Cybersecurity Threats in Aviation and Aerospace

Note. This figure illustrates the multidisciplinary factors influencing insider cybersecurity threats in aviation and aerospace, including motivations, impacts, empirical examples, technological evolution, and the central role of sustainability and ethics in organizational response. The diagram emphasizes the need for integrated strategies that address both technical and human elements to ensure resilience and security.

2. Discussion

2.1 Motivational Dynamics and Behavioral Risk in Aviation Insider Threats: Toward an Integrated Security Framework

The complexity of modern organizational arson in aviation is not limited to the technical tools and methods employed by insiders but also encompasses the diverse and often overlapping motivations that drive individuals to commit these acts (Jones, 2024). Traditional criminological frameworks, such as Routine Activity Theory, provide valuable insights into understanding this behavior by identifying the convergence of three key conditions: a motivated offender, a suitable target, and the absence of capable guardians (Thomas et al., 2024). In the context of insider threats within aviation, the motivated offender may be a disgruntled employee, a financially driven saboteur, or an ideologically committed actor, each with unique psychological and situational triggers. The suitable target is typically the organization's sensitive data or critical digital infrastructure, while the absence of capable guardians may result from insufficient monitoring, weak access controls, or gaps in organizational oversight (Burrell et al., 2022; ICAO, 2022).

For example, an employee who has been passed over for promotion may develop increasing resentment, eventually gaining access to sensitive databases containing flight plans and passenger information. Motivated by feelings of injustice, the individual might deliberately alter or delete critical records, forcing the aviation organization to scramble for recovery and potentially compromising flight safety (Jones, 2024). In another scenario, a financially desperate insider could be lured into selling proprietary information about airport security protocols to a competitor or malicious external actor, causing irreparable harm to the organization's security posture and, by extension, public safety (Said, 2024).

Modern digital arsonists in aviation do not act impulsively; their behaviors are often deliberate and calculated, leveraging their deep understanding of organizational systems to inflict maximum damage while concealing their tracks (Gimarelli, 2025). This calculated approach makes detection and prevention particularly challenging, necessitating the implementation of sophisticated monitoring systems and a robust culture of security awareness among all employees (Nobles, 2022). Their actions are frequently planned over extended periods, exploiting trust and access privileges to bypass traditional security controls and maximize operational disruption (Jones, 2024).

The motivations behind insider threats are as varied as the individuals themselves, ranging from personal grievances and workplace dissatisfaction to financial gain and ideological causes (ICAO, 2022; Majzoub, 2025). Behavioral indicators such as withdrawal from team activities, sudden changes in work patterns, or unauthorized attempts to access sensitive systems often precede malicious actions, underscoring the significance of ongoing behavioral analytics and proactive management (Nobles, 2022; Thomas et al., 2024). Aviation organizations must

remain vigilant to these warning signs, integrating psychological profiling and risk assessment into their security strategies to identify potential threats before they escalate (Ukwandu et al., 2022).

Addressing the human element is as critical as implementing technical safeguards, as even the most advanced security technologies can be circumvented by a determined insider with legitimate access (Malik, 2025). Creating a workplace environment that fosters transparency, open communication, and employee well-being can mitigate the feelings of disenfranchisement and discontent that often motivate insider threats. Additionally, regular training and awareness programs help employees recognize and report suspicious behavior, reinforcing the collective responsibility for organizational security (ICAO, 2022; Nobles, 2022).

Ultimately, a comprehensive approach to insider threat mitigation in aviation requires the integration of legal, technical, and behavioral strategies, ensuring that all potential vulnerabilities are addressed (Leppard Law Firm, 2024). By understanding the complex interplay of motivation, opportunity, and organizational culture, aviation organizations can develop more resilient defenses against the evolving threat posed by insider digital arsonists (Jones, 2024; Gimarelli, 2025).

2.2 Empirical Depth Gap: Real-World Aviation Insider Threat Examples

Real-world incidents provide the clearest illustration of the risks posed by insider threats in aviation and aerospace. Case studies reveal the operational, financial, and reputational consequences that arise when insider threats materialize, demonstrating the necessity of robust, multidisciplinary strategies for detection, prevention, and response. These examples underscore the profound impact insider actions can have on safety and organizational resilience, offering compelling evidence for integrating technical, behavioral, and legal approaches in aviation cybersecurity.

Example 1: The Horizon Air Q400 Incident (2018)

The 2018 Horizon Air Q400 incident, in which a ground service agent exploited privileged access to commandeer an aircraft, illustrates the catastrophic potential of insider threats. This event exposed critical vulnerabilities in physical and procedural security, emphasizing the need for behavioral monitoring and robust employee support systems to detect and mitigate insider risks before they escalate (FBI Seattle, 2018). The aftermath of the incident prompted aviation organizations worldwide to reevaluate their access controls and employee screening processes. Such proactive measures are essential for preventing similar breaches and safeguarding operational continuity and public safety.

Example 2: The Boeing Data Breach (2023)

Enabled by malicious insiders and compromised credentials, this breach resulted in the loss of sensitive operational data and significant reputational harm, highlighting the necessity of robust access controls and continuous monitoring. The incident disrupted internal processes, forcing the organization to reassess its data protection strategies and strengthen its incident response capabilities (Baran, 2024). Ultimately, the breach demonstrated how insider-enabled cyberattacks can undermine trust, compromise competitive advantage, and necessitate ongoing vigilance across all levels of aviation operations.

Example 3: The Seattle-Tacoma Airport Ransomware Attack (2024)

Triggered by insider negligence, this attack led to widespread operational disruptions, underscoring the significance of comprehensive cybersecurity training and effective incident response protocols. The ransomware infection disrupted flight scheduling and passenger processing, compelling the airport to divert flights and revert to manual procedures (Slauson & Fox, 2024). This case illustrates the cascading effects of insider-related incidents and the critical need for aviation organizations to foster a culture of security awareness and preparedness.

2.3 Cybersecurity as Organizational Firefighting: Strategic Defense Against Digital Arson in Aviation

The challenge of countering insider threats in aviation often conceptualized as digital arson, has led cybersecurity leaders to pursue strategies that integrate technical, behavioral, and organizational solutions, much like modern firefighting requires a coordinated response to contain and extinguish fires (Jones, 2024). This approach recognizes that technical controls alone are insufficient to address the complexity and unpredictability of insider threats, which exploit digital vulnerabilities and human trust (Malik, 2025; Nobles, 2022).

A foundational element of this strategic defense is the implementation of stringent access controls, which restrict employee access to only the information and systems essential for their specific roles (ICAO, 2022; Plachkinova & Knapp, 2023). By minimizing the attack surface, organizations reduce opportunities for malicious or negligent insiders to cause harm while also lowering the risk of accidental data exposure. The principle of least privilege is

especially critical in aviation, where unauthorized access to operational or safety-critical systems can have immediate and far-reaching consequences for public safety and organizational integrity (ICAO, 2022; FAA, 2024).

Real-time monitoring and anomaly detection technologies, such as User and Entity Behavior Analytics (UEBA), serve as digital equivalents of fire alarms and smoke detectors, providing early warning of potential threats. These systems analyze patterns of user activity to identify deviations that may signal malicious intent or compromised credentials. For example, an employee accessing sensitive flight data at unusual hours or downloading large volumes of passenger information without a legitimate business purpose would trigger alerts, enabling security teams to intervene before a breach escalates.

However, technical defenses alone cannot fully address the human dimensions of insider risk. Aviation organizations must also foster a culture of security awareness and accountability, ensuring that all employees understand the significance of safeguarding sensitive information and the potential consequences of insider threats (ICAO, 2022; Malik, 2025). Regular training programs and clear communication about security policies help employees recognize and report suspicious behavior while also reinforcing the collective responsibility for organizational security (Nobles, 2022).

An effective insider threat mitigation strategy also requires robust incident response planning, ensuring that organizations can quickly contain and recover from security incidents (Georgiadou et al., 2021). This includes establishing protocols for investigating potential threats, preserving evidence, and communicating with relevant stakeholders, as well as conducting post-incident reviews to identify lessons learned and improve future responses (Leppard Law Firm, 2024; ICAO, 2022). Regularly updating these response plans in light of new threats and organizational changes further strengthens resilience and ensures that aviation organizations remain prepared for evolving insider risks (Malik, 2025).

The integration of these technical, behavioral, and organizational measures creates a comprehensive defense posture that addresses the full spectrum of insider threats, from accidental missteps to deliberate sabotage (Jones, 2024). By viewing cybersecurity as a form of organizational firefighting, aviation organizations can better protect their critical infrastructure, safeguard public safety, and maintain operational resilience in an increasingly complex and interconnected digital environment. This multidisciplinary approach not only enhances detection and mitigation capabilities but also fosters a proactive security culture that is essential for adapting to the evolving nature of insider threats in aviation.

Ultimately, the metaphor of firefighting underscores the necessity of vigilance, preparedness, and collaboration as aviation organizations work to anticipate, detect, and extinguish digital fires before they can spread and cause irreparable harm (Gimarelli, 2025). Just as fire departments train rigorously for diverse emergency scenarios, aviation cybersecurity teams must engage in continuous scenario planning and drills to ensure rapid, coordinated responses to insider threats (Burton, 2023). This proactive stance not only minimizes the likelihood and impact of incidents but also fosters a resilient organizational culture where every member understands their role in safeguarding critical systems and sensitive data (ICAO, 2022).

2.4 The Escalating Impact of Unaddressed Insider Threats in Aviation

When aviation organizations fail to proactively manage insider threats, especially those driven by malicious intent, the consequences extend far beyond immediate technical or financial damage (Jones, 2024). Insider incidents, often conceptualized as digital arson, disrupt operational continuity, erode stakeholder trust, and compromise the safety and integrity of critical aviation infrastructure. The financial consequences of insider threats in aviation can be profound, encompassing immediate and long-term losses that affect operational budgets, crisis response, and ongoing organizational resilience (Ponemon Institute & DTEX, 2025; Majzoub, 2025; Gimarelli, 2025).

The reputational fallout from insider attacks is particularly severe in the aviation sector, where public confidence and regulatory compliance are paramount (ICAO, 2022). Clients may abandon the organization, top talent may seek opportunities elsewhere, and the brand's image may never fully recover, even after technical systems have been restored. This loss of trust can have long-term implications for market share, partnerships, and the ability to attract and retain skilled personnel (Majzoub, 2025).

Beyond financial and reputational harm, insider threats inflict significant psychological and emotional distress on employees and leaders alike (Labree et al., 2010). The unpredictable nature of digital sabotage fosters a pervasive sense of vulnerability and anxiety, undermining morale and hindering productivity across the organization. In high-stakes environments like aviation, where teamwork and reliability are essential, this erosion of psychological safety can compromise operational effectiveness and increase the risk of further incidents.

The persistent threat of insider-driven crises also exhausts cybersecurity teams, diverting resources from proactive security planning to constant crisis management (Majzoub, 2025). This reactive posture diminishes an organization's capacity to anticipate emerging threats, innovate, and adapt to evolving risks, leaving it increasingly vulnerable to future attacks. As a result, the cumulative effect is a weakened security posture and a workforce that is less resilient in the face of adversity.

Addressing these multifaceted challenges requires a holistic approach that integrates advanced technical safeguards, robust access controls, and a strong organizational culture rooted in transparency, accountability, and psychological support (ICAO, 2022; Malik, 2025). Regular training and awareness programs help employees recognize and report suspicious behavior, reinforcing the collective responsibility for organizational security (Burton, 2022; Pincus, 2025). By fostering a culture of continuous improvement and open communication, aviation organizations can better anticipate, detect, and mitigate insider threats, thereby safeguarding their assets and the broader public interest.

Ultimately, the metaphor of the organizational arsonist serves as a potent reminder that the most destructive threats often come from within, exploiting trust and privilege to inflict chaos (Jones, 2024). Only by embracing a multidisciplinary, human-centric strategy can aviation organizations hope to extinguish the fires of digital sabotage and build a more secure, resilient future. This integrated approach not only enhances detection and mitigation capabilities but also fosters a proactive security culture that is essential for adapting to the evolving nature of insider threats in aviation.

2.5 Integrating Sustainability and Ethics: Strategic Imperatives for Aviation Cybersecurity Leadership

Embedding sustainability and ethical considerations into aviation cybersecurity is a strategic imperative that extends beyond regulatory compliance and technical safeguards (Rafi, 2022). Aviation organizations must recognize that sustainable cybersecurity practices not only protect sensitive data and critical infrastructure but also enhance business resilience, operational continuity, and long-term stakeholder value. By prioritizing ethical business conduct, organizations can build trust with passengers, regulators, and partners while mitigating risks that could otherwise lead to reputational harm, financial loss, or legal liability (ABB, 2024).

A robust approach to sustainable cybersecurity begins with the alignment of organizational values with industry best practices, ensuring that every decision, from technology adoption to incident response, reflects a commitment to responsible stewardship (Rafi, 2022). Leaders must foster a culture of transparency and accountability, where employees are empowered to report suspicious activities without fear of retaliation, and where ethical dilemmas are addressed through clear, consistent policies. This cultural foundation not only reduces the likelihood of insider threats but also strengthens the organization's ability to adapt to evolving risks and regulatory expectations (ICAO, 2022).

From a business perspective, integrating sustainability and ethics into cybersecurity requires ongoing investment in employee training, advanced monitoring technologies, and cross-functional collaboration (ABB, 2024). Regular training programs ensure that all personnel, from frontline staff to executives, understand their roles in safeguarding sensitive information and maintaining operational integrity. Continuous monitoring and behavioral analytics enable organizations to detect anomalies early, respond swiftly to incidents, and minimize disruptions to critical aviation services.

Effective change management is essential for embedding these values across the organization, particularly as new technologies and threats emerge (Cheraghi et al., 2023; Rafi, 2022). Leaders must communicate the significance of sustainability and ethics at every level, aligning cybersecurity initiatives with broader business objectives such as customer trust, regulatory compliance, and market competitiveness. By involving diverse stakeholders in the planning and implementation of security measures, organizations can identify potential risks, anticipate resistance, and develop strategies that balance security needs with ethical considerations (ABB, 2024).

Ultimately, sustainable and ethical cybersecurity is not merely a compliance exercise but a source of competitive advantage for aviation organizations (Rafi, 2022). Companies that embrace these principles are better positioned to anticipate and respond to emerging threats, maintain the confidence of regulators and customers, and contribute to the long-term viability of the aviation industry. By integrating sustainability and ethics at the core of their cybersecurity strategies, aviation leaders can ensure that their organizations remain secure, responsible, and prepared for the challenges of an increasingly complex digital landscape.

2.6 Navigating Technological Evolution: Change Management and Resilience in Aviation Cybersecurity

The rapid advancement of digital technologies presents opportunities and challenges for aviation organizations striving to maintain robust cybersecurity postures (Industrial Cyber, 2024). As innovations such as AI, autonomous

systems, and advanced data analytics are integrated into aviation operations, the complexity and interconnectivity of organizational systems increase exponentially. This change heightened complexity not only enhances operational efficiency and passenger experience but also expands the attack surface available to external and internal threat actors (FAA, 2024; Georgiadou et al., 2021).

Effective change management is paramount for aviation organizations seeking to adapt to these technological shifts while mitigating the associated risks. Leaders must ensure that the adoption of new systems and processes is accompanied by comprehensive training, updated security protocols, and clear communication channels for all stakeholders (Rafi, 2022; Weir, 2025). By involving employees at every level in the planning and implementation of technological changes, organizations can foster a culture of adaptability and vigilance, reducing resistance to change and increasing the likelihood of successful cybersecurity integration (Ukwandu et al., 2022).

Continuous learning and professional development are essential components of a resilient cybersecurity strategy in the face of rapid technological evolution (Kupiek, 2023). Aviation and aerospace organizations must invest in ongoing education for their workforce, ensuring that all personnel are equipped to recognize and respond to emerging threats, such as sophisticated phishing campaigns or AI-driven cyberattacks. Regular scenario-based training and simulation exercises can further enhance preparedness, enabling teams to identify vulnerabilities and refine incident response procedures before real-world incidents occur (Pincus, 2025).

The dynamic nature of the aviation industry, coupled with the global scope of its operations, requires organizations to remain agile in their approach to technological change (Industrial Cyber, 2024). International collaboration, information sharing, and the harmonization of security standards across jurisdictions are critical for addressing the systemic risks posed by insider threats and digital sabotage (ICAO, 2022). By prioritizing adaptability, continuous improvement, and cross-functional collaboration, aviation organizations can build a resilient cybersecurity ecosystem capable of withstanding the challenges of a rapidly evolving digital landscape (Georgiadou et al., 2021).

Ultimately, the successful integration of new technologies into aviation cybersecurity depends on a holistic approach that balances technical innovation with human-centric strategies and robust change management practices (Errida et al., 2021). Aviation leaders must remain vigilant, proactive, and committed to fostering a culture of security awareness and accountability throughout the organization. This forward-thinking mindset not only safeguards critical infrastructure and sensitive data but also ensures the long-term resilience and competitiveness of the aviation sector in an era of unprecedented technological change.

2.7 Strategic Resilience in Aviation and Aerospace: Navigating Global Uncertainty and Multidimensional Risks

Aviation organizations operate in an increasingly complex and volatile global landscape, where economic volatility, political instability, and geopolitical tensions present persistent challenges to operational continuity and business resilience (Industrial Cyber, 2024). These external pressures can disrupt supply chains, alter regulatory environments, and introduce new security threats, all of which demand agile and adaptive organizational strategies. The unpredictability of global events, such as trade disputes, sanctions, and abrupt policy shifts, requires aviation leaders to anticipate risks and prepare for a wide range of potential scenarios that could affect everything from flight operations to supply chain logistics (Garcia-Blanco, 2022).

Effective risk management in this context extends beyond traditional cybersecurity and insider threat mitigation, encompassing broader considerations of economic exposure, regulatory compliance, and stakeholder confidence. Aviation organizations must invest in robust scenario planning and business continuity frameworks to ensure they can respond swiftly to external shocks, whether these arise from geopolitical conflicts, natural disasters, or shifts in international trade policy (Klenka, 2021; ICAO, 2022). By fostering a culture of continuous learning and adaptability, organizations can empower their workforce to identify early warning signs and implement proactive measures that safeguard critical operations and infrastructure (Kupiek, 2023).

The interconnected nature of the aviation industry amplifies the impact of global risks, as disruptions in one region can rapidly cascade through international networks, affecting passenger safety, cargo logistics, and organizational reputation. For example, a sudden escalation of geopolitical tensions may lead to airspace closures, increased regulatory scrutiny, or restrictions on cross-border data flows, all of which can impair the seamless operation of global aviation systems (Federal Aviation Administration [FAA], 2024; Industrial Cyber, 2024). Aviation leaders must therefore maintain a global perspective, collaborating with international partners, regulators, and industry stakeholders to share intelligence, align standards, and coordinate responses to emerging threats (Garcia-Blanco, 2022).

Clear and transparent communication is essential for maintaining stakeholder confidence and employee morale during periods of heightened uncertainty (Burton, 2023). Organizations should regularly update their risk

assessments, ensure that contingency plans are current and actionable, and provide ongoing training to staff at all levels. By embedding resilience into every layer of the organization, from frontline operations to executive decision-making, aviation enterprises can navigate the complexities of the global risk environment with greater confidence and effectiveness (ICAO, 2022; Kupiek, 2023).

Ultimately, strategic resilience in aviation requires a holistic approach that integrates technical, organizational, and human-centric strategies to address immediate threats and long-term vulnerabilities. By anticipating change, adapting to new realities, and fostering a culture of preparedness, aviation organizations can protect their assets, maintain operational continuity, and uphold their commitment to safety and security in an era of unprecedented global uncertainty (Garcia-Blanco, 2022).

3. Conclusion: Aviation and Aerospace Cybersecurity in the Digital Age: A Multidisciplinary Conclusion

The challenge of insider cybersecurity threats in aviation is no longer merely a technical issue but a complex, multidimensional crisis that demands a holistic and adaptive response. Deliberate misuse of internal access can trigger cascading failures across digital infrastructure, threatening safety, continuity, and national security (Jones, 2024; Lauzier, 2025). Recent incidents such as the Horizon Air Q400 unauthorized flight, the Boeing data breach, and the Seattle-Tacoma Airport ransomware attack demonstrate the severe operational, financial, and reputational consequences of insider actions or compromised credentials (Baran, 2024; Lambert, 2025; Slauson & Fox 13 Seattle Digital Team, 2024).

Traditional technical defenses alone are insufficient to counter the evolving tactics of insider threats in aviation. Instead, a multidisciplinary approach is essential, one that integrates advanced technological safeguards—such as artificial intelligence, behavioral analytics, and real-time monitoring, with robust legal frameworks, ethical leadership, and a strong organizational culture (ICAO, 2022; Malik, 2025; Plachkinova & Knapp, 2023). Behavioral insights allow organizations to identify and mitigate risks before they escalate, while continuous training and awareness programs empower employees to recognize and report suspicious activities, reinforcing a collective commitment to security (Nobles, 2022; Pincus, 2025).

Looking ahead, the rapid pace of technological change in aviation, including the adoption of artificial intelligence, the Internet of Things (IoT), and autonomous systems, will continue to expand the attack surface and introduce new vulnerabilities (FAA, 2024; Georgiadou et al., 2021; Industrial Cyber, 2024). The increasing presence of digitally native employees, such as Generation Z and Millennials, and the heightened risk associated with senior executives and board members due to their extensive access, require tailored training and ongoing awareness initiatives (GlobeNewswire, 2024; Majzoub, 2025). The aviation sector must also anticipate emerging risks from deepfake technology, AI-driven cyberattacks, and the integration of next-generation air traffic management and in-flight connectivity solutions, all of which present new opportunities for insider exploitation (Industrial Cyber, 2024; Ukwandu et al., 2022).

Strategic resilience in aviation cybersecurity will depend on predictive threat modeling, scenario-based training, and innovative monitoring methods, such as User and Entity Behavior Analytics (UEBA), to detect anomalies and respond swiftly to potential insider incidents. Collaboration, within organizations and across the broader industry, is essential for sharing intelligence, harmonizing standards, and building a global culture of cybersecurity (ICAO, 2022). Regulatory bodies are tightening requirements, mandating robust access controls, incident response planning, and continuous risk assessments to safeguard critical infrastructure and sensitive data (FAA, 2024; Leppard Law Firm, 2024).

By embracing these principles, aviation and aerospace organizations can better anticipate, detect, and mitigate insider threats, ensuring the safety, reliability, and resilience of operations in an era of unprecedented digital transformation. The future of aviation cybersecurity will be defined by its ability to adapt, innovate, and collaborate, integrating technical, legal, and behavioral strategies while fostering a culture of vigilance and accountability (Burton, 2023; Jones, 2024). This comprehensive approach not only safeguards critical assets and public safety but also upholds the industry's commitment to operational excellence in the face of evolving insider threats.

References

ABB. (2024). Coming full circle: Introducing *ABB EcoSolutions*. https://global.abb/group/en/sustainability/ecosolutions

Baran, G. (2024, May 13). Boeing confirms LockBit hackers demanded $200 million ransom after 2023 data breach. *Cyber Security News*: Ransomware. https://cybersecuritynews.com/boeing-confirms-lockbit-demanded/

Bovenizer, N. (2024, May 10). Boeing confirms 2023 $200m ransomware demand. *Airport Technology*. https://www.airport-technology.com/news/boeing-confirms-2023-hack-200m-ransomware/

Burrell, D. N., Lewis, E. J., & Richardson, K. (2023). Adaptive marketing, management strategy, and technology innovation in beverage and hospitality markets. *International Journal of Innovation in the Digital Economy (IJIDE), 14*(1), 1–10. https://doi.org/10.4018/IJIDE.330524

Burton, S. L. (2023). Cybersecurity risk: The business significance of ongoing tracking. In D. N. Burrell (Ed.), *Transformational interventions for business, technology, and healthcare* (pp. 245–268). IGI Global. https://doi.org/10.4018/979-8-3693-1634-4.ch015

Burton, S. L. (2022). *Cybersecurity leadership from a telemedicine/telehealth knowledge and organizational development examination* (Publication No. 29066056) [Doctoral dissertation, Northcentral University]. ProQuest Dissertations & Theses Global.

Butaka, G. (2021, November 17). Human error in cyberspace. ISACA. https://www.isaca.org

Cheraghi, R., Ebrahimi, H., Kheibar, N., & Sahebihagh, M. H. (2023). Reasons for resistance to change in nursing: An integrative review. *BMC Nursing, 22*, 310. https://doi.org/10.1186/s12912-023-01460-0

Cybersecurity & Infrastructure Security Agency. (n.d.). Defining insider threats. Author. https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

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. https://doi.org/10.1016/j.cose.2021.102516

Davies, N. (2025, June 9). Cybersecurity in aviation: Rising threats and modernization efforts. *Secureworld*. https://www.secureworld.io/industry-news/aviation-cybersecurity-threats

Eleimat, M., & Őszi, A. (2025). Cybersecurity in aviation: Exploring the significance, applications, and challenges of cybersecurity in the aviation sector. *Periodica Polytechnica Transportation Engineering, 53*(2), 169–183. https://doi.org/10.3311/PPtr.37153

Errida, A., & Lotfi, B. (2021). The determinants of organizational change management success: Literature review and case study. *International Journal of Engineering Business Management, 13*, 1–15. https://doi.org/10.1177/18479790211016273

FBI Seattle. (2018, November 9). FBI completes investigation into August 2018 unauthorized flight from Seattle-Tacoma Airport. https://www.fbi.gov/contact-us/field-offices/seattle/news/press-releases/fbi-completes-investigation-into-august-2018-unauthorized-flight-from-seattle-tacoma-airport

Federal Aviation Administration. (2024). *NextGEN annual report 2024*. https://www.faa.gov/nextgen/NextGen-Annual-Report-2024.pdf

Garcia-Blanco, B. (2022, May 16). Threathunt 2030: Future cybersecurity threats for aviation sector. European Union Aviation Safety Agency (EASA). https://www.easa.europa.eu/community/topics/threathunt-2030-future-cybersecurity-threats-aviation-sector

Garg, N., & Sharma, N. (2025). Does gratuitous behaviour promote workplace nonviolence? Exploring the mediating role of constructive deviance. *International Journal of Emerging Markets, 20*(4), 1686–1704. https://doi.org/10.1108/IJOEM-07-2022-1129

Gelles, M. G. (2021). Insider threat prevention, detection, and mitigation: Building an insider threat program. In J. R. Meloy & J. Hoffmann (Eds.), *International handbook of threat assessment* (2nd ed., pp. 669–693). Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0037

Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. *Big Data Analytics, 1*(1), 6. https://doi.org/10.1186/s41044-016-0006-0

Gimarelli, C. (2025). The hidden threats in the skies: Cybersecurity lessons from recent aviation crises. *Cyentia Institute*. https://www.cyentia.com/the-hidden-threats-in-the-skies-cybersecurity-lessons-from-recent-aviation-crises/

GlobeNewswire. (2024, March 5). 2024 data exposure report: Companies at risk of data loss driven by changing workforce, AI usage, and source code exfiltration. *Author.* https://www.globenewswire.com/news-release/2024/03/05/2840495/0/en/2024-Data-Exposure-Report-Companies-at-Risk-of-Data-Loss-Driven-by-Changing-Workforce-AI-Usage-and-Source-Code-Exfiltration.html

Industrial Cyber. (2024, January 30). Aviation industry faces rising cybersecurity risks as new technologies drive adoption, says Aviation ISAC survey. *Author*. https://industrialcyber.co/reports/aviation-industry-faces-rising-cybersecurity-risks-as-new-technologies-drive-adoption-says-aviation-isac-survey/

International Civil Aviation Organization. (2022). *ICAO insider threat toolkit*. https://www.icao.int/Security/securityculture/Documents/Insider%20threat%20toolkit.EN.pdf

Jones, L. A. (2024). Unveiling human factors: Aligning facets of cybersecurity leadership, insider threats, and arsonist attributes to reduce cyber risk. *Security, 8*(2), 44–63. https://doi.org/10.21511/sec.8(2).2024.04

Jones, L. A. (2020). *Reputation risk and potential profitability: Best practices to predict and mitigate risk through amalgamated factors* (Publication No. 28152966) [Doctoral dissertation, Northcentral University]. ProQuest Dissertations & Theses Global.

Kizilcan, S., & Mizrak, K. C. (2022). Cyber attacks in civil aviation and the concept of cyber security. *International Journal of Disciplines Economics & Administrative Sciences Studies, 8*(47), 745–748.

Klenka, M. (2021). Aviation cyber security: Legal aspects of cyber threats. *Journal of Transportation Security, 14*(3–4), 177–195. https://doi.org/10.1007/s12198-021-00232-8

Krull, K. E. (2016, August). *The threat among us: Insiders intensify aviation terrorism* (PNNL-25689). U.S. Department of Energy. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-25689.pdf

Kupiek, M. (2023). Revisiting organizational change management (OCM): A context-sensitive and dynamic approach of change. In M. Kupiek & R. A. Brandmeier (Eds.), *The digital transformation of Georgia* (pp. 91–106). Springer. https://doi.org/10.1007/978-3-031-26451-1_7

Labree, W., Nijman, H., van Marle, H., & Rassin, E. (2010). Backgrounds and characteristics of arsonists. *International Journal of Law and Psychiatry, 33*(3), 149–153. https://doi.org/10.1016/j.ijlp.2010.03.004

Lambert, K. (2025, September 18). Hackers demand $6 million for files stolen from Seattle airport operator in cyberattack. AP: *The Seattle Times*. https://apnews.com/article/seattle-airport-cyberattack-ransomware-rhysida-95cd980a9f45112f0fdce488233eec9c

Lauzier, J. G. (2025). Insurance design and arson-type risks. *Annals of Actuarial Science, 19*(1), 126–139. https://doi.org/10.1017/S1748499524000186

Lekota, P., & Coetzee, M. (2019). Cybersecurity incident response for the sub-Saharan African aviation industry. In *2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICABCD.2019.8851011

Leppard Law Firm. (2024, December 20). Evaluating insider threats under the Computer Fraud and Abuse Act and US federal law. *Author*. https://leppardlaw.com/federal/computer-crimes/evaluating-insider-threats-under-the-computer-fraud-and-abuse-act-and-us-federal-law/

Leppard Law Firm. (2021). Analyzing the role of cybersecurity negligence in damage cases under federal law. *Author*. https://leppardlaw.com/federal/computer-crimes/analyzing-the-role-of-cybersecurity-negligence-in-reckless-damage-cases-under-federal-law/

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Implementing cyber-security measures in airports to improve cyber-resilience. In *2018 Global Internet of Things Summit (GIoTS)* (pp. 1–6). IEEE. https://doi.org/10.1109/GIOTS.2018.8534575

Mahdi, A. K., & Assim, M. I. S. A. (2025). Managing unprofessional behavior in the workplace: An organizational psychology perspective. *International Journal of Science Academic Research, 6*(1), 9023–9024.

Majzoub, M. S. (2025, June 27). Insider threats are the trojan horse of cybersecurity in the AI era. *Forbes.* https://www.forbes.com/councils/forbestechcouncil/2025/06/27/insider-threats-are-the-trojan-horse-of-cybersecurity-in-the-ai-era/

Malik, H. (2025, March 19). Why the aviation industry needs robust cybersecurity strategies. *Access Intelligence*. https://www.satellitetoday.com/cybersecurity/2025/03/19/why-the-aviation-industry-needs-robust-cybersecurity-strategies/

Mimecast. (2024). *Annual data exposure report 2024*. https://www.mimecast.com/resources/white-papers/annual-data-exposure-report-2024/

National Insider Threat Special Interest Group. (2021). Legal counsel support to insider threat program. Author. https://www.nationalinsiderthreatsig.org/itrmresources/Laws%20And%20Regulations%20Related%20To%

20Insider%20Threats-Espionage-Fraud%2012-15-14.pdf

National Academies of Sciences, Engineering, and Medicine. (2025). *Actions from federal government needed to alleviate air traffic controller staffing shortages at many facilities*. https://www.nationalacademies.org/news/2025/06/actions-from-federal-government-needed-to-alleviate-air-traffic-controller-staffing-shortages-at-many-facilities-says-new-report

Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA: Journal of Business and Public Administration, 13*(1), 49–72. https://doi.org/10.2478/hjbpa-2022-0003

Osborne, C., & Thompson, J. A. (2024). Shedding new light for nurses: Enhancing pressure injury prevention across skin tones with sub-epidermal moisture assessment technology. *Journal of Advanced Nursing, 80*(6), 2450–2460. https://doi.org/10.1111/jan.16040

Petkauhas, V. (2023, November 15). Boeing breach: LockBit leaks 50 GB of data. *Cybernews.* https://cybernews.com/news/boeing-data-leak-lockbit-ransomware/

Pincus, E. (2025, January 27). The ultimate guide to security awareness training. *INFOSEC*. https://www.infosecinstitute.com/resources/security-awareness/ultimate-guide/

Plachkinova, M., & Knapp, K. (2023). Least privilege across people, process, and technology: Endpoint security framework. *Journal of Computer Information Systems, 63*(5), 1153–1165. https://doi.org/10.1080/08874417.2022.2128937

Ponemon Institute & DTEX. (2025). *Cost of insider risks global report*.

Ponemon-Sullivan Report. (2023). *Cost of insider risks global report – 2023*. https://ponemonsullivanreport.com/2023/10/cost-of-insider-risks-global-report-2023/

Quinn, S., Waheduzzaman, W., & Djurkovic, N. (2025). Impact of organizational culture on bullying behavior in public sector organizations. *Public Personnel Management, 54*(2), 184–208. https://doi.org/10.1177/00910260241287619

Rafi, T. (2022, June 9). Why sustainability is crucial for corporate strategy. *World Economic Forum*. https://www.weforum.org/agenda/2022/06/why-sustainability-is-crucial-for-corporate-strategy/

Said, S. (2024). Emerging aviation security challenges: Preparing for 2025. *LinkedIn*. https://www.linkedin.com/pulse/emerging-aviation-security-challenges-preparing-2025-safieeldin-said-3wawf

Slauson, T., & FOX 13 Seattle Digital Team. (2024, September 13). Cyberattack that brought down Sea-Tac Airport systems was ransomware. *FOX 13 Seattle*. https://www.fox13seattle.com/news/sea-labor-day-cyberattack-ransomware

Smith, G. (2024, December 10). Insider threat statistics: (2025's most shocking trends). *StationX*. https://www.stationx.net/insider-threat-statistics/

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, A., & 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

U.S. Equal Employment Opportunity Commission. (n.d.). Facts about retaliation. *Author.* https://www.eeoc.gov/facts-about-retaliation

United States Department of Justice. (2021). *Justice manual: Computer Fraud and Abuse Act (CFAA)*. *Author*. https://www.justice.gov/jm/jm-9-48000-computer-fraud

Weber, L. (2025). Annex 17 and related aviation security measures. In J. R. Huang (Ed.), *The Elgar companion to the law and practice of the International Civil Aviation Organization* (pp. 456–470). Edward Elgar Publishing. https://doi.org/10.4337/9781035315987.00039