International Journal of Management Studies and Social Science Research

Types of Insider Threats in the Aviation Sector

Gubara Said Hassan (Assistant Professor)
Department of Political Science, Sultan Qaboos University, Oman.

Aaisha Rashid AL Zaabi (MA)
Department of Political Science, Sultan Qaboos University, Oman.

DOI: https://doi.org/10.56293/IJMSSSR.2025.5902

IJMSSSR 2025
VOLUME 7
ISSUE 6 NOVEMBER - DECEMBER **ISSN: 2582 – 0265**

Abstract: The aviation sector is a critical component of global transportation and commerce, yet it remains highly vulnerable to insider threats that can compromise safety, security, and operational continuity. This study explores and categorizes the various types of insider threats within the aviation industry, emphasizing both intentional and unintentional actors. Using qualitative research methodology, the paper synthesizes findings from case studies, incident reports, and regulatory frameworks issued by the International Civil Aviation Organization (ICAO), International Air Transport Association (IATA), and national aviation security agencies. The analysis identifies five principal types of insider threats: malicious insiders driven by ideological, financial, or personal motives; coerced or manipulated employees; negligent or complacent staff; contractors with privileged access; and cyber insiders exploiting digital vulnerabilities. The study reveals that these threats, which also include sabotage, theft of intellectual property, fraud, and espionage. are often facilitated by systemic weaknesses such as insufficient background checks, poor information-sharing, and limited behavioral monitoring. The paper concludes that a comprehensive, multi-layered security strategy—integrating personnel vetting, cybersecurity, psychological assessment, and organizational culture—is essential to mitigating insider risks. By mapping insider typologies and their enabling factors, this research contributes to the development of proactive, intelligence-led aviation security frameworks that enhance resilience and safeguard public confidence in the global aviation system.

Keywords: Aviation security; Insider threats; Human factors; Airport safety; Cybersecurity; Risk management; Organizational resilience; ICAO regulations

Introduction

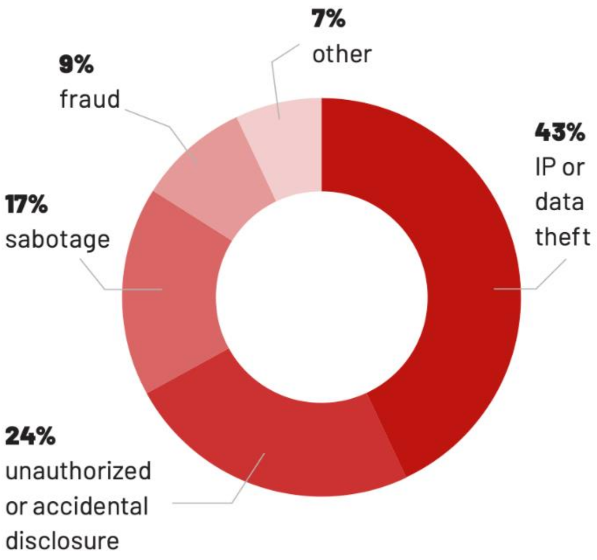
The insider threats, according to (Ophoff, Jensen, Smith, Porter, & Johnston, 2014), are a major information security issue marked by people inside an organization abusing their legal access privileges to carry out hostile actions. These risks are especially difficult as insiders know the system architecture and security flaws of the company, which gives them a good position to abuse the information systems (Hamin, 2000). Moreover, the International Civil Aviation Organization (ICAO) defines insider threat as a potential danger that arises from individuals inside an organization (International Civil Aviation Organization (ICAO), 2022). Different points of view exist on the definition of insider threats. Insider threats, according to (Theoharidou , Kokolakis , Karyda , & Kiountouzis, 2005), are the use of privileges by persons with access rights that violates an information security policy of an entity. Incorporating any activities by insiders that compromise the data, procedures, or resources of an organization widen this concept (Pfleeger, Predd, Hunker, & Bulford, 2010). Insider threats, according to (Sarkar, 2010), may be unintentional as well as malicious a perspective agreed upon by (Carroll, 2006). Schultz (2002) contends, nonetheless, that insider threats should only apply to deliberate harmful actions.

Insider threats consistently present a significant challenge across multiple sectors, particularly in those dealing with sensitive data, such as aviation, banking, and investment (Price & Forrest, 2017). These types of threats are responsible for roughly 34% of all data breaches, with incidents related to insiders costing companies an average of $11 million for each occurrence (Ponemon Institute, 2020). The aviation industry is particularly at risk due to its dependence on critical infrastructure and the possibility of catastrophic results from a successful insider attack. Recent investigations highlight the complexity and seriousness of insider-related activities. For example, 32% of malicious insider incidents were associated with unusual reconnaissance behavior, while 12% involved the deliberate circumvention of security measures, both of which significantly complicate detection and mitigation efforts. Furthermore, in certain instances, insider threats, like cyberattacks, may arise from insider actions, further exacerbating the risks. This underscores the necessity for strong security protocols and a proactive strategy to address insider threats in high-risk sectors such as aviation (DTEX, 2024).

Types of Insider Threats

Researchers at Carnegie Mellon University examined 118 instances of insider events, classifying them into specific insider risks: Information Technology (IT) sabotage, theft for monetary gain, and theft for competitive advantage (Caputo, Maloof, & Stephens, 2009). A recent review of insider investigations further highlights the distribution of related threat categories. As shown in the infographic below, insider risks comprise intellectual property theft (43%), unauthorized disclosure (24%), sabotage (17%), fraud (9%), and other malicious activities (7%). These incidents frequently arise from departing employees taking sensitive or proprietary information with them—76% of leaving employees take non-sensitive proprietary data, while 15% take sensitive intellectual property. Profiling these insider threats are essential for comprehending their behaviors and objectives. By categorizing insider threats into these types—sabotage, intellectual property theft, fraud, and espionage—it not only helps identify the risks but also supports the development of targeted security strategies to effectively mitigate the threats (DTEX, 2024).

Chart (1): Breakdown of insider investigation



Source: (DTEX, 2024)

The aviation industry encounters a variety of malicious threats, including terrorism, criminal activities, and insider attacks from disgruntled or mentally unstable employees (Kelly, 2021). With the adoption of Information Communication Technology (ICT) tools, cybersecurity issues have escalated, exposing weaknesses in software-driven systems (Ukwandu, et al., 2021). As the aviation sector progresses with electronically enabled aircraft, drones, and advanced airports, it becomes increasingly vital to tackle these security challenges.

Sabotage

Sabotage involves intentional actions taken by an insider with the goal of damaging an organization's assets, which can include physical infrastructure, data, and reputation. It is defined as "the intentional destruction or disruption of an organization's resources" (Cappelli, Moore, & Trzeciak, 2012). It is distinct from other insider threats like theft or espionage because it is primarily motivated by a desire to cause damage rather than to achieve personal gain. The motivations for sabotage often arise from feelings of retribution, discontent with the organization, or ideological beliefs (Cole & Ring, 2005). From the aviation preservative, sabotage refers to deliberate actions aimed at harming or disrupting aircraft, airport facilities, or associated services, thereby endangering the safety of aviation. Such actions may involve destroying aircraft, interfering with navigation systems, or placing hazardous items onboard (Flight Safety Foundation (FSF), 2024). These activities are classified as criminal offenses under the Montreal Convention and U.S. law (18 U.S.C. § 32) due to their ability to jeopardize lives and operations. The Flight Safety Foundation recognizes sabotage as a major threat (Archived U.S. Department of Justice , 2024). In the aviation sector, where consistency and safety are critical, the repercussions of sabotage can be disastrous, leading to potential operational interruptions and even loss of life.

Disgruntled employees often play a key role in incidents of sabotage. Utilizing their extensive understanding of an organization's systems and infrastructure, they have the potential to inflict considerable damage. This could involve the erasure of essential data, the alteration of operational systems, or even the introduction of harmful software (Wright, 2017). In the aviation sector, for instance, such actions could entail interfering with air traffic control systems, disrupting maintenance schedules, or embedding malicious code in operational software.

The aviation industry's dependence on complex and interconnected systems makes it especially susceptible to sabotage. Misconfigurations within essential Information Technology (IT) infrastructure, like exposed Virtual Network Connections (VNCs), heighten these vulnerabilities. A recent investigation revealed that unrestricted access via open VNCs enabled attackers to take control of critical systems, gain access to sensitive operational information, and manipulate equipment, potentially jeopardizing human safety (DTEX, 2024). These vulnerabilities underscore the significant dangers that sabotage poses to aviation operations, where even slight disruptions can have extensive consequences.

Sabotage is frequently motivated by perceived grievances or conflicts within the workplace. Insiders may act out of resentment or a wish for revenge, leveraging their technical knowledge to circumvent security protocols and exploit weaknesses in the organization (Shaw, Ruby, & Post, 1998). As noted by Cole & Ring (2005), sabotage in fields such as aviation can result in immediate and catastrophic consequences, disrupting flight operations, endangering passenger safety, and damaging the organization's reputation.

The rising occurrence of insider sabotage highlights the necessity for proactive security strategies such as regular risk assessment and threat detection. Insights from the DTEX (2024) Insider Risk Investigations Report indicate that individuals with advanced Information Technology (IT) skills frequently take advantage of inadequate security measures, like unsecured remote access points. These individuals are perpetually on the lookout for chances to breach systems, which makes it imperative for organizations to focus on maintaining security standards, carry out regular risk assessments, and educate employees to identify and address insider threats.

Theft of Intellectual Property (IP)

When valuable data, trade secrets, or sensitive data held in digital systems is taken or shared without authorization, it is referred to as Information Technology (IT) theft of intellectual property (IP) (Hossain, et al., 2021) Research outcomes, marketing plans, product designs, source code, and any other information that gives a competitive advantage may all be considered examples of this kind of data. According to Al-Harrasi, et al.. (2021), this kind of theft often occurs when individuals, such as contractors, employees, or trusted partners, abuse their legitimate access to copy, transfer, or otherwise misuse confidential data. While some insiders may intentionally steal data to further their own interests or the interests of a competing company, others may unintentionally expose confidential information by disregarding security procedures.

The unlawful acquisition of intellectual property (IP) has become a significant issue across various industries, particularly in the aviation field. Insiders may acquire access to sensitive information, such as sophisticated technological designs, patents, or secret procedures, eroding a company's competitive advantage and potentially harming broader security interests. These employees may then utilize the stolen information to acquire employment with other companies or rise competing research programs (Meneghetti & Perrotta , 2022) Insider-driven intellectual property theft has high implications for businesses and national security since contemporary aviation depends on innovatory technology that may frequently be adapted for both commercial and military uses (Seamans, Sohn, & Sands, 2024).

The dual-use aspect of these advancements amplifies the possible repercussions of insider leaks. When crucial designs or systems of an aviation company can be repurposed for military use, the effects of compromised technology go far beyond mere financial loss, impacting international security and adherence to regulations. Additionally, the aviation sector's growing reliance on digital platforms increases this vulnerability, as valuable information can be illegally copied or transmitted with few physical traces. Therefore, enhanced cybersecurity measures and strong internal controls are essential to deter and detect such breaches promptly.

The World Intellectual Property Organization (WIPO) provides worldwide assistance for initiatives to preserve intellectual property in aviation and other sectors. WIPO, which operates under the United Nations umbrella, provides guidelines, capacity-building initiatives, and dispute resolution services to promote worldwide intellectual property frameworks (World Intellectual Property Organization (WIPO), 2021). These resources contribute to conditions in which corporations may more effectively deal with insider threats. Aviation participants, especially, gain advantages by synchronizing their intellectual property protection approaches with widely accepted international standards, considering the global aspects of innovation and manufacturing in this field (Homoliak, Toffalini, Guarnizo, Elovici, & Ochoa, 2019)

The aviation industry depends on a wide range of intellectual property assets, including distinctive aircraft designs, manufacturing methods, and advanced operational systems. These assets are appealing targets for adversaries looking to circumvent the substantial financial and time investments required for innovation (Nurse et al., 2014). Insiders frequently contribute significantly to these breaches, motivated by factors such as financial rewards, coercion, or revenge (Shaw, Ruby, & Post, 1998). The sector's engagement in both commercial and military projects heightens these risks, making it a common target for espionage and sabotage (Moore, Cappelli, & Trzeciak, 2008). Recent findings from DTEX (2024) highlight the seriousness of this problem, indicating that 43% of insider threat investigations in 2023 were related to intellectual property or data theft. Departing employees posed a particularly notable threat, with 15% being identified as having taken sensitive information, including vital intellectual property (IP). Other industries such as technology, pharmaceuticals, and critical infrastructure, which have similar technological dependencies, also reported elevated levels of IP theft, further illustrating the vulnerabilities faced by all these critical sectors.

One of the difficulties in addressing intellectual property (IP) theft stems from the authorized access that insiders generally have, which complicates detection. Typical methods involve utilizing personal email accounts or unauthorized applications for the transfer of proprietary information. This requires the implementation of advanced monitoring tools that can detect unusual access behaviors or significant data transfers (Silowash et al., 2012; Bishop, 2002). DTEX (2024) points out several warning signs, such as insiders using various webmail accounts not associated with corporate domains, an uptick in email activity related to outside businesses, and visiting external company sites connected to competitors or threats.

Fraud

Fraud constitutes a major insider threat, defined by individuals taking advantage of their authorized access to steal from their organizations. This can manifest in various ways, such as altering financial statements, generating fraudulent invoices, or misappropriating funds. The main drivers of fraud typically include personal greed, financial stress, or a conviction that they can breach organizational trust without being caught (Bishop, 2002). In contrast to sabotage, which aims to damage the organization, fraud is mainly concerned with individual gain at the expense of the company. Insiders who engage in fraud frequently have an in-depth knowledge of the organization's financial operations, allowing them to go undetected for long periods and inflict significant financial damage (Cole & Ring, 2005).

In the aviation industry, insider fraud manifests in various ways, such as financial fraud, procurement fraud, and the falsification of maintenance or safety documentation (Greitzer & Frincke, 2010). Procurement fraud typically involves insiders modifying contracts to benefit certain suppliers in return for unlawful payments. Financial fraud entails the misappropriation of funds or inflation of expenses. Altering maintenance records presents a significant risk in aviation, where safety is critical. Such actions can lead to disastrous outcomes, threatening both aircraft safety and operational dependability (Randazzo & Cappelli, 2004). Fraud in the aviation sector is particularly damaging, as it not only leads to financial losses but also erodes safety, efficiency, and public confidence (Cappelli, Moore, & Trzeciak, 2012).

The reasons for insider fraud in the aviation sector often center on the pursuit of financial rewards. This can occur when individuals meet their financial goals through unethical actions, such as embezzling funds or receiving bribes for personal gain (Shaw, Ruby, & Post, 1998). In certain instances, insiders may engage in fraudulent activities due to external pressures or personal issues (Nurse et al., 2014). Additionally, the aviation industry's dependence on outside contractors and suppliers renders it vulnerable to collusion between insiders and external parties, a practice known as procurement fraud. In this scenario, insiders work alongside external entities to manipulate contracts or artificially raise prices for their mutual advantage (Moore, Cappelli, & Trzeciak, 2008).

According to the International Civil Aviation Organization (ICAO) classification, fraud is frequently perpetrated by those categorized as "Exploited Insiders" or "Collaborators." These individuals may act with different degrees of malice, ranging from being coerced into actions to intentionally working with outside parties. At the highest level of risk, "Malicious Insiders" might deliberately scheme and carry out fraud for personal gain or to benefit others. In contrast, "Negligent Insiders" or "Complacent Insiders," who are lower on the intent scale, may unintentionally enable fraud by not following established policies or by granting access to more malicious individuals. Recognizing these risk categories is crucial for formulating targeted strategies to reduce risk within the aviation industry International Civil Aviation Organization (ICAO, 2022).

The difficulty of identifying fraud in aviation organizations arises from the intricate nature of their financial and operational systems. Insiders frequently possess authorized access to the systems they misuse, complicating the ability to differentiate between harmful actions and legitimate ones. Furthermore, the fragmented organization of many aviation companies—operating across various locations with multiple stakeholders—can hinder the timely detection of fraud, allowing schemes to continue for long durations (Bishop, 2002).

Espionage

Espionage poses a significant insider threat, defined by the deliberate and systematic gathering of confidential information by individuals who have authorized access. Often motivated by ideological beliefs, coercion, or financial incentives, espionage is especially harmful in sectors where strategic data, such as trade secrets, military strategies, or proprietary technologies, are of great value (Cole & Ring, 2005). In the aviation industry, espionage has historically hindered development, as evidenced during the Cold War when it influenced international relations and the advancement of civil aviation (Kleve, 2020). Currently, modern espionage tactics encompass cyber-enabled methods like GPS and ADS-B spoofing, which can provide false location data to systems, resulting in threats such as hijacking or the disruption of airspace monitoring (Kožović & Đurđević, 2021).

In the field of aviation, espionage refers to the unlawful gathering of sensitive information or technology, frequently carried out by insiders, including engineers, military contractors, or high-level executives. These insiders, who have legitimate access, may be recruited by foreign intelligence agencies or rival companies looking for crucial aviation technologies. Unlike external cyberattacks that breach security perimeters, insider espionage takes advantage of authorized access, making typical cybersecurity measures ineffective (Bishop, 2002). This type of activity is often deliberate and planned over the long term, frequently remaining undetected, as insiders engage in careful measures to avoid raising suspicion while they take essential information (Silowash et al., 2012).

The consequences of espionage in the aviation sector are far-reaching. Groups classified as Advanced Persistent Threats (APTs), often backed by government entities, specifically focus on the IT infrastructure of aviation to acquire intellectual property and intelligence (Ukwandu, et al., 2021). For example, the rise of unmanned aerial vehicles (UAVs) has increased the scope of threats, allowing for both physical and cyber assaults on vital aviation systems and operations. Meanwhile, non-state players, including organized crime groups like the Sinaloa Cartel or extremist groups like Al Qaeda, are using more advanced strategies to attack aviation infrastructure and networks. These organizations represent a significant risk to vital supply chains, air traffic control systems, and operations data by using sophisticated hacking tools and worldwide connections (Krame, Vivoda, & Davies, 2023). Although critical infrastructure generally benefits from protection at the state level, non-state actors and private aviation organizations continue to be susceptible to these developing dangers (Horváth, 2024).

The reasons behind espionage in the aviation sector often include financial incentives, alignment with certain ideologies, or pressure from external forces. The fragmented structure of aviation companies and their dependence on outside contractors further complicate this problem, as individuals within these organizations may collaborate with external parties to gain access to critical technologies. For example, procurement processes can be skewed to benefit foreign interests, which jeopardizes national security (Moore, Cappelli, & Trzeciak, 2008). The potential dangers go beyond monetary setbacks and include threats to operational safety, a diminishing competitive edge, and considerable harm to reputation (Shaw, Ruby, & Post, 1998).

The challenge of identifying espionage stems from the insider's authorized access to critical systems and information. This access complicates the task of distinguishing between normal activities and malicious actions. Additionally, espionage efforts frequently focus on aviation technologies that can be used for both civilian and military purposes, heightening their strategic value to hostile entities (Randazzo & Cappelli, 2004). Recent developments in cybersecurity measures have sought to detect unusual behaviors among insiders, yet the advanced techniques employed by state-sponsored actors and the insider capability to integrate into legitimate processes continue to pose significant obstacles (Silowash et al., 2012).

Exemplary Case Studies of Insider Threats in the Aviation Sector

This subsection specifically highlights case studies of insider threats within the aviation sector. It explores real incidents to illustrate how insiders have exploited their access, the circumstances involved, and the impact these threats have had on aviation security and safety.

Table (1): Case studies of Insider Threat in The Aviation Sector

Date	Incident	Cause	Context	Impact	References
1982	Japan Airlines flight 350	Pilot deliberately crashed the plane	Mental health and job insecurity	24 killed	(Nori, 2020)
1985	Air India 181/18229	A bomb exploded on a flight between Montreal and London. It may be linked with an explosion the same day at Tokyo-Narita airport.	Possibly extremist Sikh group Babbar Khalsa30	329 killed A five-step screening process (including x- ray, visual, explosives) was instituted in Canada A Canadian government enquiry was finished in 2010 and concluded, among other things, that security flaws remained, particularly in respect to cargo.	(Aviation Safety Network., 2024) (Summers, 2005)

1994	FedEx Flight 705 Hijacking Attempt	Personal grievances and financial motive	Employee attempted to hijack and crash a plane for insurance payout	Crew subdued hijacker; led to emphasis on mental health screening in aviation roles	(Price & Forrest, 2016).
2015	Germanwings Flight 9525 Crash	Pilot\u2019s severe mental health issues	Co-pilot locked out captain and deliberately crashed plane. Mental illness. Self-reporting of symptoms and a fear or losing his license without sufficient insurance means the mental illness of the pilot was not known	Mandatory two-person cockpit rule; enhanced mental health monitoring 150 killed Changes to Lufthansa policy, and various countries' national laws, stipulating that two pilots need to be in the cockpit at any one time. Calls for more psychological testing of pilots.	(Evans, 2016) (Marquez & Calvo, 2018) (Pinsky, Jeffrey, Berry, Chesanow, & Pinals, 2020) (Kelly, 2021)
2015	Kenya Airways Employee Terrorist Plot	Radicalization of aviation staff	Employee attempted to smuggle explosives onto a flight	Advanced verification and monitoring systems; increased international intelligence sharing	(ADHIAMBO, 2016) (International Civil Aviation Organization (ICAO) , 2016) (Omweno, 2022)
2020	Shooting down of Ukraine International Airlines flight PS752	Shot down by Iranian missiles by mistake	Heightened tensions following killing of Iranian General Soleimani. The plane was flying close to a military center.	176 people killed	(Kelly, 2021)

Conclusion

The aviation sector, as a foundation of global mobility and economic interconnectivity, faces a complex and evolving array of tremendous security challenges, among which insider threats remain among the most insidious and difficult to detect. These threats continue to be a significant vulnerability in the aviation industry, influenced by a range of motivations including financial gain, ideological convictions, mental health concerns, and dissatisfaction within the workplace. Historical incidents show that the aviation sector must constantly evolve and enhance its security measures to counter such security challenges and threats. This study has examined the fundamental types of insider threats that affect aviation operations—ranging from intentional malicious acts, such as sabotage, theft of intellectual property, fraud, and espionage, to unintentional behaviors resulting from negligence, complacency, or inadequate training. The findings underscore that insiders, by virtue of their legitimate access to sensitive information, systems, and restricted areas, pose a security risk that external actors alone cannot replicate.

A key insight emerging from the analysis is that insider threats in aviation are multifaceted and extend beyond the stereotypical image of the "rogue employee." They include categories such as disgruntled staff, radicalized individuals, financially motivated insiders, coerced personnel, and unwitting participants manipulated through social engineering or cyber exploitation. Moreover, the convergence of physical and cyber domains has intensified the threat landscape, as digital vulnerabilities can now be exploited by insiders to compromise operational integrity, passenger safety, and national security.

Effective mitigation, therefore, requires a holistic, intelligence-driven, and multi-layered approach that integrates human resource management, behavioral analysis, cybersecurity, and regulatory oversight. The study highlights the importance of continuous vetting, real-time behavioral monitoring, and cultivating a culture of security awareness among all aviation personnel. Collaboration between airlines, airport authorities, intelligence agencies, and international regulatory bodies such as ICAO and IATA is crucial for harmonizing detection and response strategies across jurisdictions. ICAO regulations are international standards and recommended practices (SARPs) established by the International Civil Aviation Organization (ICAO) to ensure the safety, security, and efficiency of global air travel. These regulations are detailed in the 19 Annexes to the Chicago Convention, covering a wide range of topics from pilot licensing and aircraft maintenance to airport infrastructure and air traffic control. States must conform to these standards, which form the basis for national aviation laws and ensure a consistent and safe experience for passengers worldwide

In addition, to effectively manage and reduce risks, proactive approaches such as thorough psychological evaluations, robust monitoring systems, and international collaboration are crucial. Organizations should emphasize the creation of comprehensive internal controls and the development of a workplace culture that addresses insider threats to protect not only financial assets but also human lives and national security. Furthermore, establishing clear and enforceable policies, improving training and awareness initiatives, and investing in cutting-edge cybersecurity technologies can greatly enhance aviation security. Future policies should emphasize preventive strategies, resilience, and adaptability, ensuring that aviation organizations are equipped to quickly address emerging threats and neutralize them before they can cause harm.

In conclusion, insider threats in aviation cannot be eliminated entirely, but they can be systematically reduced through proactive risk management, data-driven screening, and continuous employee engagement. The evolving nature of these threats necessitates an adaptive security framework that balances vigilance with trust, technology with human judgment, and regulation with organizational culture. Future research should focus on predictive analytics, AI-based behavior detection, and cross-sector lessons to enhance resilience in aviation security systems. Ultimately, understanding and addressing insider threats is not merely a security imperative. Rather, it is a fundamental prerequisite for maintaining public confidence in the global aviation ecosystem

References

1. Adhiambo, L. D. (2016). *Effect of terrorism on air transport industry in Africa: A case study of Kenya*. University of Nairobi Research Archive. http://hdl.handle.net/11295/99809
2. Archived U.S. Department of Justice. (2024). *Aircraft sabotage (18 U.S.C. 32)*. https://www.justice.gov/archives/jm/criminal-resource-manual-2-aircraft-sabotage-18-usc-32?utm_source=chatgpt.com
3. Aviation Safety Network. (2024, December 30). *ASN aircraft accident Boeing 707-300C A6-DPA Mogadishu International Airport (MGQ)*. https://asn.flightsafety.org/asndb/327181

4. Caputo, D., Maloof, M., & Stephens, G. (2009). Detecting insider theft of trade secrets. *IEEE Security & Privacy, 7*(6), 14–21.
5. Carroll, M. D. (2006). Information security: Examining and managing the insider threat. In *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development* (pp. 156–158). ACM.
6. DTEX. (2024). *2024 insider risk*. DTEX.
7. Evans, A. (2016). *Germanwings accident 24 March 2015: An overview*. Bureau d'Enquêtes et d'Analyses (BEA). https://bea.aero/en/
8. Flight Safety Foundation. (2024). *Sabotage and intentional acts*. https://flightsafety.org/safety-issue/sabotage-intentional-acts/?utm_source=chatgpt.com
9. Hamin, Z. (2000). Insider cyber-threats: Problems and perspectives. *International Review of Law, Computers & Technology, 14*(1), 105–113.
10. Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys, 52*(2), 1–40.
11. Horváth, I. (2024). The newest aspect of industrial espionage: Cyber threats from UAVs to non-state actors. *Rendvédelem*. https://bm-tt.hu/wp-content/uploads/2024/04/2024_2_Illes-Horvath.pdf
12. Hossain, S., Rahman, H., Hosen, S., Seo, C., Cho, H., & Rahman, S. (2021). Intellectual property theft protection in IoT based precision agriculture using SDN. *Electronics*, *10*(8), 1987.
13. International Civil Aviation Organization (ICAO). (2016). *Windhoek Declaration on Aviation Security and Facilitation in Africa: Ministerial conference*. ICAO.
14. Kelly, L. (2021). *Threats to civilian aviation since 1975*. Institute of Development Studies. [https://hdl.handle.net/20.500.12413/15952] (https://hdl.handle.net/20.500.12413/15952).
15. Kleve, K. L. (2020). Fearing the eye in the sky: How the fear of espionage affected the development of civil aviation during the Cold War. *The International Journal of Intelligence, Security, and Public Affairs, 22*(3), 307–327.
16. Kožović, D., & Đurđević, D. (2021). Spoofing in aviation: Security threats on GPS and ADS-B systems. *Vojnotehnički Glasnik, 69*(1), 1–15.
17. Krame, G., Vivoda, V., & Davies, A. (2023). Narco drones: Tracing the evolution of cartel aerial tactics in Mexico's low-intensity conflicts. *Small Wars & Insurgencies, 34*(6), 1095–1129.
18. Marquez, D., & Calvo, G. (2018). Human factors and insider threats: A case study approach in aviation. *International Journal of Aviation Management, 4*(2), 150–165.
19. Meneghetti, A., & Perrotta, P. (2022). *Aviation law*. International Comparative Legal Guides (ICLG). [https://maples.com/wp-content/uploads/2023/11/AV22_Chapter-18_Ireland.pdf] (https://maples.com/wp-content/uploads/2023/11/AV22_Chapter-18_Ireland.pdf)
20. Nori, H. (2020). The use of drones in counterterrorism: Emerging technologies and their implications for international law. *London Met Repository*. [https://repository.londonmet.ac.uk/6132/] (https://repository.londonmet.ac.uk/6132/)
21. Omweno, E. N. (2022). Legal, regulatory and technical responses to terrorism in the aviation industry in Kenya. *Science Mundi, 2*(1), 1–21.
22. Ophoff, J., Jensen, A., Smith, J. S., Porter, M., & Johnston, K. (2014). A descriptive literature review and classification of insider threat research. In *Proceedings of Informing Science & IT Education Conference* (pp. 211–223). InSITE.
23. Pfleeger, S. L., Predd, J., Hunker, J., & Bulford, C. (2010). Insiders behaving badly: Addressing bad actors and their actions. *IEEE Transactions on Information Forensics and Security, 5*(1), 169–179.
24. Pinsky, H., Jeffrey, G., Berry, M., Chesanow, C., & Pinals, D. (2020). Psychiatry and fitness to fly after Germanwings. *The Journal of the American Academy of Psychiatry and the Law, 48*(1), 65–74.
25. Ponemon Institute. (2020). *Cost of insider threats global report*. https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2020/12/UK-VR-Proofpoint-Report-2020-Cost-of-Insider-Threats.pdf
26. Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report, 15*(3), 112–133.
27. Schultz, E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security,

21*(6), 526–531.

28. Seamans, R., Sohn, E., & Sands, D. (2024). Technology adoption and innovation: The establishment of airmail and aviation innovation in the United States, 1918–1935. *Strategic Management Journal*, 1–25.
29. Summers, C. (2005). Deadly puzzle remains a mystery. *BBC News*. http://news.bbc.co.uk/2/hi/americas/4344051.stm
30. Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO 17799. *Computers & Security, 24*(6), 472–484.
31. Ukwandu, E., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., & Ben-Farah, M. A. (2021). Cyber-security challenges in aviation industry: A review of current and future trends. *Information, 12*(4), 146.
32. World Intellectual Property Organization (WIPO). (2021). *World intellectual property indicators 2021*. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2021.pdf