Risk Homeostasis Theory applied to Aviation Security

Risk Homeostasis Theory (RHT)

Risk Homeostasis Theory (RHT) also known as "risk compensation", developed by Gerald J.S. Wilde, posits that individuals have a target level of risk they are willing to accept to maximize the overall expected benefit from an activity. Consequently, they adjust their behaviour to maintain this level, via a regulating process (homeostasis) that keeps the outcome close to the target, by compensating from disturbing external influences, regardless of changes in safety measures or regulations (Wilde, 1998, 2014).

When applied to aviation security, this theory suggests that improvements in security measures or regulations may lead to compensatory behaviours by individuals, potentially offsetting the intended security benefits. These individuals range from customers, or passengers for aviation, to ground staff, air crew, regulators, inspectors, including their respective families and friends that could impact on their assessment of the overall benefit they could expect from any activity. This dynamic is crucial to understand for developing efficiency, cost-effectiveness and sustainability in aviation security management strategies.

Introduction

Aviation security aims to protect passengers, crew, and aircraft from unlawful interference, including terrorism, hijacking, and other criminal activities. The application of risk homeostasis theory to aviation security involves examining how individuals and organizations respond to enhanced security measures and processes, and whether these responses maintain a constant level of perceived risk.

Technological Advancements and Risk Compensation

Technological advancements in aviation security, such as Advanced Imaging Technology (AIT), Artificial Intelligence (AI), biometric identification systems, facial recognition, and fingerprint scanning, have significantly improved threat detection capabilities, threat analysis, as well as accuracy and efficiency of passenger, crew, and staff identification.

However, according to RHT, these advancements may lead to risk compensation behaviours. For instance, passengers might become less vigilant about their own security, relying heavily on technology to detect threats (Hunter, 2002). Similarly, security personnel might be overly dependent on the technology, become complacent, assuming that advanced systems will catch all potential threats, thereby reducing their own vigilance, attentiveness and thoroughness during security checks and procedures, and potentially missing threats that the technology cannot detect (Hunter, 2002).

Advanced imaging technology, including full-body scanners, has enhanced the ability to detect concealed weapons and explosives. However, the reliance on these technologies can lead to a false sense of security among passengers and security personnel. Passengers and staff may feel that the technology will catch any threats, leading them to be less observant of their surroundings, their environment, and less likely to report suspicious behaviours and activities. Those events that appear to be abnormal, unusual, strange and could be a good indicator or precursor for security analysts, as explained by the International Civil Aviation Organization (ICAO) when promoting the reporting of security occurrences by all individuals (ICAO, 2022).

Regulatory Frameworks and Behavioral Adjustments

Regulatory frameworks play a critical role in aviation security. International organizations like ICAO for States, and the International Air Transport Association (IATA) for airlines, set global standards for security measures. Since the last two decades, IATA has been promoting the concept of Security Management System or SeMS (IATA, 2020) for implementing these global standards with the most efficient, economic, sustainable, and risk-based approach for air transport operators. However, RHT suggests that as these regulations become more stringent, individuals and organizations might adjust their behaviours to maintain their individual target levels of risk. For example, stricter security protocols and procedures might lead to increased attempts at circumventing these measures by those with malicious intent, such as insiders, as they adapt to the new security environment (Wilde, 2014).

The implementation of stringent security measures, such as the requirement for passengers to remove shoes and belts during security screening, has probably be judged effective in reducing certain types of threats by the authorities imposing such measures. However, these measures can also lead to frustration and non-compliance among passengers not sharing the same threat assessment point of view. They may seek ways to bypass the security process, resulting in increased processing and queuing times at security checkpoints. This non-compliance, or resistance to compliance, can create vulnerabilities in the security system, as passengers may attempt to smuggle prohibited items through alternative means (Wilde, 2014).

Another example with the introduction of liquid restrictions in carry-on luggage that has effectively reduced the risk of liquid explosives. However, this measure has also led to increased attempts to smuggle prohibited items through other means, demonstrating the compensatory behaviours predicted by RHT (Wilde, 2014). Moreover, passengers may attempt to hide prohibited items in their checked luggage or use other creative methods to bypass the restrictions, creating new challenges for security personnel and aviation security in general.

When commercial entities apply the very same “creativity” in bypassing security restrictions or measures, for example in mis-declaring dangerous items such as Lithium batteries, leading to the unsafe air transport of dangerous goods, the consequences for aviation operations could be catastrophic.

Human Factors and Security Culture

Human factors are integral, or even essential to aviation security. Security personnel must be well-trained and vigilant to effectively implement security measures, and to remain the active ground guardians and sources of information for detecting ground vulnerabilities. However, RHT implies that as security measures become more advanced, there might be a decline in the perceived need for human vigilance, or even importance of the human pillar within the security system. This can lead to a false sense of security and reduced situational awareness among security staff (Hunter, 2002).

To counteract this, fostering a strong security culture within the aviation industry is essential. ICAO (2021) shared a collection of initiatives, tools and visual supports developed by many States, Organizations, and International Associations, as part of the Year of Security Culture (YOCS) initiative. Continuous training and awareness programs can help maintain high levels of vigilance and proactive threat detection among security personnel (Hunter, 2002). IATA (2020) shared a set of short, and free of charge videos about security awareness and security reporting, which remain available in 13 different languages, for making aviation security culture accessible, free of charge, to more than 90% of the population using their native languages.

The role of human factors extends to the design and implementation of security technologies. User-friendly interfaces and ergonomic designs ensure that security personnel can effectively operate advanced systems without compromising performance. Additionally, multiple new platforms of exchange among aviation security practitioners and experts are available for reinforcing the *raison d’être* of security culture, fostering information and practical tools sharing and developing global trust, IATA (2022) facilitated the human exchanges via a SeMS Aviation Community open to all security managers, supervisors, regulators, consultants for sharing advanced tools for enhancing Security Culture and Security Management implementation among aviation eco-system.

Challenges with Occurrence and Incident Reporting

In the context of security occurrence and incident reporting, human factors, risk compensation and Risk Homeostasis Theory (RHT) play a critical role. Security professionals must conduct risk analyses on all reported occurrences to determine which occurrences could be elevated to the status of an incident, fully aware of all the implications and consequences of officially declaring a security incident.

Beyond the corporate and organization's responsibility to identify which occurrence (or threat or vulnerability) has materialized into a security incident – representing a genuine, **realized risk** that activates internal regulating mechanisms (homeostasis) including the deployment of immediate treatment and protective measures - serious incidents must also be reported to the appropriate authorities. Such mandatory reporting of security incidents may introduce additional external and regulatory pressures, including potential reputational exposure.

This potential negative exposure is amplified when Operators outsource the implementation of their security measures to External Service Providers (ESPs). As highlighted in the Public Position Paper on the Reporting of Aviation Security Occurrences and Incidents (IATA, 2025-1), outsourcing does **not** transfer an Operator's official responsibility for reporting security incidents, even when occurrences are initially detected and reported by an ESP. Challenges may arise when:

- ESPs report directly to the authorities what they *perceive* to be an incident on behalf of their clients (the Operators), but without applying the same risk-assessment processes used by the Operators, and - more importantly - without informing their clients beforehand; or

- Conversely, ESPs refrain from reporting occurrences to their clients because doing so could affect contractual relationships or perception of performance.

Once again, the intended security benefits of mandatory and timely reporting of serious security incidents to the appropriate authorities may be undermined or offset by compensatory behaviours by both the ESPs and the Operator's security professionals when reporting and analysing security occurrences.

To limit such risk-compensation effects, the official reporting of security incidents to authorities should be carried out only by Operators (not by ESPs acting on their behalf) and limited to "serious" security incidents duly assessed by Operator's security professionals. The reporting deadlines for serious security incidents should allow sufficient time to conduct proper risk assessments (a few days). In addition, other (non-serious) security incidents could be reported when they remain open beyond a defined period (e.g. 30 days). All incidents that have been resolved and closed are history, useful for performance measurements, but not worth for official reporting.

Conclusion

Risk Homeostasis Theory (RHT) provides a valuable framework for understanding the dynamic responses to aviation security evolving threats and measures. While technological advancements and stringent regulations are still considered as essential for enhancing security, it is crucial to recognize and address the potential for compensatory behaviours. By fostering a strong security culture and maintaining high levels of vigilance and involvement among security personnel, the aviation industry can better manage the balance between perceived and actual risks, ensuring the global safety and security of all stakeholders.

With this objective in mind, IATA (2024) launched a new **SeMS Certification Program** intended to support mature aviation stakeholders willing to demonstrate dynamic, effective management and robust delivery of security and security culture. In addition, IATA (2025-2) continuously publishes **Public Position Papers** on topics ranging from Risk Management to Hold Baggage Reconciliation (HBR), Recognition of Equivalence (RoE) and One-Stop Security (OSS), Reporting of Aviation Security Occurrences and Incidents, Aircraft Operator Security Programme (AOSP) and Supplementary State Procedures (SSPs), Cargo Security or the threat of Improvised Incendiary Devices to Aviation, in addition to its traditional guidance material, tools and resources.

References

- Hunter, D. R. (2002). Risk perception and risk tolerance in aircraft pilots. *Office of Aerospace Medicine, Federal Aviation Administration*. Risk Perception and Risk Tolerance in Aircraft Pilots
- IATA (2020), Security Management System (SeMS), https://www.iata.org/en/programs/security/security-management-system-sems/
- IATA (2022), SeMS Aviation Community, SeMS Aviation Community | Microsoft Teams (contact aviationsecurity@iata.org for access)
- IATA (2024), SeMS Certification Program, https://www.iata.org/en/services/certification/operations-safety-security/security-management-systems-sems/
- IATA (2025-1), Reporting of Aviation Security Occurrences and Incidents, https://www.iata.org/contentassets/1998554ac6624b97a2de8418938eaade/2025-reporting-of-aviation-security-occurrences-and-incidents-april-2025.pdf
- IATA (2025-2), Public Position Papers, https://www.iata.org/en/programs/security/position-papers-press-releases/
- ICAO (2021), The Year of Security Culture, https://www.icao.int/Security/Security-Culture/Pages/default.aspx
- ICAO (2022), Guidance on Reporting of Aviation Security Occurrences and Incidents, https://www.icao.int/Security/SFP/Pages/Incident-Reporting-Guidance-and-Taxonomy.aspx
- Wilde, G. J. S. (1998), Risk Homeostasis Theory: An Overview, *Injury Prevention*, 1998;4 89-9. Risk Homeostasis Theory: An Overview
- Wilde, G. J. S. (2014), *Target Risk 3: Risk Homeostasis in Everyday Life.* PDE Publications. Target Risk 3