



Aviation Cybersecurity

Fact Sheet

Overview

The aviation industry has undergone a significant digital transformation over the past two decades, spanning everything from airline corporate operations to aircraft systems, ground infrastructure, and interconnected networks. This evolution is typified by the introduction of advanced digital technologies and solutions, including connected aircraft, tablet-based electronic flight bags, cloud-enabled operations, and data-driven decision-making, among others.

The natural replacement cycle and retirement of older, less efficient fleets ensure that this trend will continue. Furthermore, growing requirements for the collection and processing of passenger information demand robust measures to protect privacy, confidentiality, and integrity.

As a result, the airline industry increasingly relies on advanced technologies that integrate ground systems, flight operations, and predictive maintenance. Some of these technologies are critical to in-flight safety while others are essential for operational efficiency, service quality, reputation, and financial performance. The increasing use of artificial intelligence and data-driven automation in aviation operations further enhances these capabilities while also introducing new cybersecurity risks that require strong governance and oversight.

However, these advancements may also introduce new vulnerabilities. As the attack surface expands, the industry requires to strengthen the understanding of cybersecurity threats and security measures to maintain safety, reliability, and resilience.

Industry Engagement and Collaboration

IATA supports industry-wide aviation cybersecurity through advocacy, the development of standards and guidance material, and the provision of services aimed at strengthening and improving cybersecurity maturity of the industry.

In response to industry's needs, and as part of IATA's broader information security strategy, several new aviation cybersecurity expert groups are being established in 2026.

- **Aviation Cybersecurity Industry Study Group (A-SG):** serving as a unified voice and strategic coordination body for the aviation industry on cybersecurity matters, fostering collaboration across aviation industry associations to effectively engage with ICAO, state regulators, and industry standard organizations in shaping global aviation cybersecurity policies and standards.
- **International Cybersecurity Standards and Regulations Study Group (SR-SG):** serving as a central industry forum for monitoring, analyzing, sharing, and influencing global cybersecurity regulations and standards that impact aviation safety, security, and operational resilience.
- **Cybersecurity Innovation Study Group (I-SG):** designing and delivering practical, scalable solutions that enhance cybersecurity resilience across the aviation industry.
- **International Aviation Cybersecurity Crisis (ICC):** providing a rapid-response, ad-hoc coordination mechanism to share timely cybersecurity threat intelligence and enhance situational awareness during cybersecurity crisis affecting the aviation sector.

IATA actively engages with its members, industry leaders, and key stakeholders to shape and communicate its role and vision for global aviation cybersecurity. Collaboration is central to strengthening industry's resilience against evolving cyber threats. Launched in 2021 to foster the exchange of knowledge and best practices, the [Cybersecurity Strategic Partnership Program](#) provides a platform for collaboration among cybersecurity

organizations and subject matter experts (SMEs) and was further evolved in 2026 with new offerings and activities.

Moreover, recognizing the need for strengthened best-practice sharing, increased awareness, and enhanced education, IATA is expanding the training offering under the [Aviation Cybersecurity Management Diploma](#), an industry-recognized qualification designed to build expertise and leadership in aviation cybersecurity.

Aviation Cybersecurity Events

In April 2026, IATA hosted the second edition of the [World Data Symposium \(WDS\)](#) in Singapore, bringing together global aviation community to discuss the future of data, technology, and cybersecurity and to promote industry collaboration. Within the framework of the Cybersecurity Runway, discussions focused on evolving cyber threats across the aviation ecosystem, increasing interdependence between cockpit and cloud environments, multi-cloud complexities, and risks arising from the convergence of IT/O and interconnected systems as well as emerging technologies, regulatory developments, and cyber-resilience strategies. Following the symposium, IATA hosted the **Aviation Cybersecurity Forum**, an exclusive meeting for C-level leaders and senior decision-makers from IATA Member Airlines and industry partners, focused on strategic collaboration, executive-level insights, and crisis-response practices through a dedicated Cybersecurity Tabletop Exercise.

Looking ahead, the next edition of the [World Data Symposium \(WDS\)](#) and **Aviation Cybersecurity Forum** will take place in April 2027 in New Delhi, continuing to strengthen global dialogue on data-driven aviation and cybersecurity resilience.

In addition, IATA will host the first **Annual Cybersecurity Summit** in Geneva from 27 to 29 October 2026, bringing together international aviation cybersecurity experts to exchange insights on emerging threats, evolving trends, and practical approaches to enhancing cybersecurity maturity.

International Engagement and Collaboration

IATA plays an active role in shaping global aviation cybersecurity policies and regulatory frameworks. Through close collaboration with international bodies such as ICAO, IATA ensures that industry perspectives are incorporated into global standards and guidance. This includes participation in the [ICAO Cybersecurity Panel \(CYSECP\)](#) and its Working Group on Cybersecurity Threat and Risks (WGCTR) and Working Group on Cybersecurity Guidance Material (WGCGM). IATA also supports periodic revision of the [ICAO Cybersecurity Action Plan \(CyAP\)](#), and contributes to establishing the roadmap over the revision of the ICAO Annexes and documents relative to cybersecurity. Another area of involvement falls under the ICAO Trust Framework Panel (TFP) where IATA follows the work of the following groups: Identity Management, Information Security, and Trust Framework Considerations.

The [ICAO Assembly 42nd Session](#) was held in Montreal from 23 September to 3 October 2025 during which IATA contributed to discussions on global aviation priorities, including cybersecurity. As part of its engagement, IATA submitted an information paper (A42-WP/667) titled "[Industry Initiative to Adopt Cybersecurity Recognition Arrangements](#)" which highlighted the growing complexity of international cybersecurity regulations and their impact on global airline operations. The paper advocated for the adoption of recognition arrangements between States as a practical solution to reduce duplicative compliance obligations, facilitate information sharing, and optimize cybersecurity resources, serving as an interim step toward long-term harmonization.

Additionally, IATA is also part of the EUROCAE WG-72/RTCA SC-216, supporting the development of industrial standards on cybersecurity for aviation.

More information on: <https://www.iata.org/cyber-security/>