Aviation Cybersecurity

Fact Sheet

The aviation industry has undergone a significant digital transformation over the past two decades, spanning everything from airline corporate operations to aircraft systems, airport and ground infrastructure, and interconnected networks that support global air transport. This evolution is typified by the introduction of advanced digital technologies and solutions, including connected aircraft, tablet-based electronic flight bags, cloud-enabled operations, artificial intelligence, 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 and operational information demand robust measures to protect privacy, confidentiality, and integrity.

As a result, the airline industry and other aviation stakeholders increasingly rely on advanced technologies that integrate ground systems, flight operations, predictive maintenance, and business functions. Some of these technologies are critical to in-flight safety, safety-related operations, while others are essential for operational efficiency, service quality, reputation, regulatory compliance, 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, oversight, and risk management.

While digitalization delivers significant operational and business benefits, it also expands the aviation sector's cyber-attack surface and creates new opportunities for malicious actors to disrupt operations, compromise sensitive information, or affect critical systems. Maintaining safety, security, reliability, and resilience of the global air transport system therefore requires a strong and continually evolving cybersecurity posture.

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 the cybersecurity maturity of the aviation industry.

In response to evolving industry's needs, and as part of IATA's broader information security strategy, several new aviation cybersecurity study groups were established in 2026 to provide collaborative forums through which member airlines and industry stakeholders can align on priorities, share expertise, develop practical solutions, and influence the future direction of aviation cybersecurity.

- **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 the aviation 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 engagement among cybersecurity organizations, technology providers, and subject matter experts (SMEs) and was expanded in 2026 through new initiatives, services, and industry engagement activities.

Furthermore, IATA is developing the Cybersecurity Innovation Exchange (CIX) Area of Involvement (AOI) under the Strategic Partnership Program, a new collaborative framework designed to accelerate industry innovation, while ensuring alignment with aviation security, operational, and regulatory requirements. Scheduled for launch in January 2027, the CIX will provide a structured environment where cybersecurity experts from IATA member airlines and strategic partners can work together to evaluate emerging technologies, analyze industry challenges, and assess innovative solutions against defined security, operational, and business outcomes.

Recognizing the importance of knowledge sharing, workforce development, and cybersecurity awareness, IATA is expanding its training portfolio 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 the 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, the increasing interdependence between cockpit and cloud environments, the complexities of multi-cloud environments, and risks arising from the convergence of IT and OT systems, and interconnected systems as well as emerging technologies, regulatory developments, and cyber resilience strategies. Following the symposium, IATA hosted the Cybersecurity Executive 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.

IATA also hosted the inaugural Annual Cybersecurity Summit in Geneva from 28 to 29 October 2026, bringing together international aviation cybersecurity experts to exchange insights on emerging threats, evolving trends, and practical approaches to strengthening cybersecurity maturity across the industry. Discussions highlighted the growing impact of artificial intelligence on both cyber-attacks and defense capabilities, the increasing importance of cyber resilience as a measure of organizational success, the continued challenge of managing supply chain risk across a highly interconnected ecosystem, and the critical role of intelligence sharing and industry collaboration in strengthening collective cyber defense.

Looking ahead, the next edition of the World Data Symposium (WDS) and Cybersecurity Executive Forum will take place on 6-8 April 2027 in New Delhi, continuing to strengthen global dialogue on data-driven aviation and cybersecurity resilience.

Industry Policy, Standards and Guidance

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 the periodic revision of the ICAO Cybersecurity Action Plan (CyAP), and contributes to the development of roadmaps for revisions to ICAO Annexes and guidance material related to cybersecurity.

Another important 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.

Through its engagement in these expert groups, IATA contributes to the continued development of the global aviation cybersecurity framework, including future ICAO Standards and Recommended Practices (SARPs), cybersecurity guidance material, cyber threat and risk management practices, information sharing, digital identity, and capacity-building initiatives.

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

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