Aviation Cybersecurity

Fact Sheet

The aviation industry has undertaken a massive digital transformation over the past two decades, from the corporate side of the airline to the aircraft, its ground and its interconnected systems. This is typified by the introduction of far more capable digital systems, technologies and solutions, including connected aircraft, tablet-based electronic flight bags, cloud-based operations, and data-driven decision making, among others.

The natural replacement cycle, combined with pandemic-related retirements of older, less efficient aircraft, ensures that this trend will continue. Additionally, all requirements around collecting passenger data, including health information, require support in terms of privacy, confidentiality, and integrity.

Hence, the airline industry relies more and more on the latest technologies, which are extensively connected from ground systems to flight operations and predictive maintenance. Some are directly relevant to the safety of aircraft in flight, others are operationally important, and many directly impact the service, reputation, and financial health of the industry.

However, new technologies may also translate into new attack surfaces for cyber criminals and terrorists. As the attack surface increases, the industry requires a better understanding of the necessary security measures to sustain and assure safety, reliability and resilience.

Aviation Cybersecurity Strategy

IATA supports industry-wide aviation cybersecurity through advocacy, standards, and guidance material development, as well as proposing services, to enhance the information security and cybersecurity maturity of the industry.

IATA's Aviation Cybersecurity Strategy is focused on three main principles in support of the airline industry.

1. **Communities of Trust:** development of communities of trust among the different stakeholders to tackle complex challenges over aviation cybersecurity and augment resilience.
2. **Standards, Recommended Practices, and Guidance Material:** development of standards, recommended practices and guidance material for IATA, or through participation in relevant working groups of international bodies, to support the airlines with harmonization efforts of regulations as well as acceptable means of compliance.
3. **Center of Excellence and Information Exchange:** articulation and coordination of different activities and forums in support of better awareness and information exchange, and establishment of strong collaborations for increased knowledge and cross-pollination of ideas.

Industry Engagement and Collaboration

IATA engages with its members, industry leaders and stakeholders to develop and subsequently communicate IATA's role and vision in global aviation cybersecurity.

IATA established the **Cybersecurity and Resilience Management Working Group (CRMWG)** with a membership representing the IATA regions. The CRMWG is mandated to develop a cybersecurity strategy and roadmap, as well as to determine the industry's response to the current and future challenges to remain safe, secure, sustainable, and resilient to cybersecurity risks.

IATA and the International Coordinating Council of Aerospace Industries Associations (ICCAIA) established together the **Aircraft Cybersecurity eXchange Restricted FORUM (rFORUM)** to better understand the risks,

whether associated with the introduction of new technologies or those that may be shared with the original equipment manufacturers (OEMs), system suppliers, and design approval holders (DAH).

In March 2023, IATA introduced the Aviation Cybersecurity Library and published relevant guidance materials to help the industry in its effort to increase posture and maturity, as many cybersecurity regulations worldwide are being articulated, augmenting challenges to compliance in different regions. Furthermore, to support the industry, IATA launched the Aviation Cybersecurity Management Diploma in 2024, an industry-recognized qualification in aviation cybersecurity.

International Engagement and Collaboration

The Aviation Cybersecurity Strategic Partnership package was launched in 2021 to facilitate exchanges and collaboration among cybersecurity organizations and subject matter experts (SMEs). Moreover, to support the airline industry, IATA signed a Memorandum of Understanding (MoU) with EUROCONTROL to collaborate in the area of aviation cybersecurity.

IATA held the sixth edition of the Aviation Cyber Threat eXchange (3CTX) Open Forum in Montreal on 29-30 October 2024. In this by-invitation-only workshop, airlines exchanged and shared challenges over third party Cybersecurity Assurance Program (CAP). They also participated in Tabletop eXercise (TTX), with industry stakeholders, including air navigation services provider (ANSPs), OEMs, systems providers, academia and researchers as well as the broader cybersecurity community. The overall goal of the 3CTX Open Forum is two-fold: firstly, to bring cybersecurity experts closer to civil aviation and, secondly, to increase their knowledge of the civil aviation ecosystem.

In October 2025, as part of its international engagement and collaboration, IATA plans to host a Cybersecurity Day, during which international experts in the field of cybersecurity will discuss and exchange insights on the emerging challenges of the industry.

IATA is involved in the aviation cybersecurity work at ICAO, including the Cybersecurity Panel (CYSECP), currently contributing to the Working Group on Cybersecurity Threat and Risks (WGCTR), and Working Group on Cybersecurity Guidance Material (WGCGM). IATA will continue to support the yearly revision of the ICAO Cybersecurity Action Plan (CyAP), as well as 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.

IATA directly contributed to the European Strategic Coordination Platform (ESCP), an initiative led by the European Union Aviation Safety Agency (EASA). In the recent years, IATA participated in the rulemaking task over the management of information security risks, for which the EASA Opinion 03/2021 was issued in June 2021, and Commission Implementing Regulation (EU) 2023/203 was adopted in October 2022, referred as EASA Part-IS. As part of this work, IATA supported the development of the Acceptable Means of Compliance (AMC) and Guidance Material for this regulation. 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/