Aviation Cybersecurity

Fact Sheet

The aviation industry has undertaken a massive digital transformation over the past 15-20 years, 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 and solutions, such as tablet-based electronic flight bags. 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 technology 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 in order to sustain and assure safety, reliability and resilience.

Aviation Cybersecurity Strategy

IATA supports industry-wide aviation cybersecurity activities to coordinate and calibrate, through advocacy, standards, services, and guidance material development, for the most appropriate level of holistic cyber maturity for 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 resilience.
2. **Information Exchange, Standards and Recommended Practices:** articulation and coordination of different activities and forums in support of better awareness and information exchange as well as the development of standards and recommended practices and guidance material.
3. **Center of Excellence:** 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 the IATA 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 how the industry needs to respond 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).

June 2024

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.

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 in the area of aviation cybersecurity, IATA signed an MoU with the Consortium for Research and Innovation in Aerospace in Quebec (CRIAQ), the Israeli National Cyber Directorate (INCD), and EUROCONTROL.

IATA held its 4th Edition of the Aviation Cyber Threat eXchange (3CTX) Open Forum, 27-28 June 2023, in Montreal. In this by-invitation-only workshop, airlines exchanged and shared challenges over the International Incident and Crisis Management as well as participated in Tabletop eXercise (TTX), with industry stakeholders, including ANSPs, OEMS and 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.

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 following the work of the Working Group on Cybersecurity Guidance Material (WGCGM). IATA will continue to support the yearly revision of the Cybersecurity Action Plan (CyAP), establishing the roadmap over the revision of the ICAO Annexes and documents relative to cybersecurity, as well as a study on international legal instruments. 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 contributes to the EASA European Coordination Strategic Platform (ESCP) and the Rulemaking Task (RMT).0720 over the Management of information security risks, for which the EASA Opinion 03/2021 was issued in June 2021 and was adopted in June 2022 as the Commission Delegated Regulation (EU) 2022/1645. As part of this work, IATA supported the development of the Acceptable Means of Compliance (AMC) and Guidance Material for this regulation. Moreover, IATA is also part of the EUROCAE WG-72/RTCA, supporting the development of Industrial Standards on cybersecurity for aviation.

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