Aviation Cyber Security

Fact Sheet

From the corporate side of the airline to the aircraft, its ground and its interconnected systems, the aviation industry has undertaken a massive digital transformation over the past 15-20 years 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. In addition, new requirements around the collection of passenger 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 Cyber Security Strategy

IATA is supporting an industry-wide Aviation Cyber Security Strategy to enhance the industry capability in addressing this ever-evolving cyber threat.

The Aviation Cyber Security Strategy is focused on four main principles:

- **Cyber security culture**: Promoting a positive cyber security culture and raising awareness across the industry.
- **Transparency and trust**: Establishing a global approach to cyber security with a similar mindset to that which has guided aviation on safety and general security issues, including supply chain aspects.
- **Communication and collaboration**: Creating stronger relationships among players in the aviation industry and external entities to improve the development of best practices and the management of cyber security risks.
- **Workforce**: Ensuring that aviation personnel are trained to recognize and manage cyber security risks and inspire the next generation of leaders.

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 cyber security.

IATA established the **Cyber Management Working Group (CMWG)** with a membership representing the IATA regions. The CMWG is mandated to develop a cyber security strategy and roadmap for IATA to determine how the industry needs to respond to the current and future challenges to remain safe, secure, sustainable, and resilient to cyber security risks.

The **Aircraft Interconnected Systems Cyber Security Steering Group (AISCS- SG)** is an informal group that aims to prioritize and develop different activities for cyber resilience of the aircraft, ground and the interconnected systems related to flight safety and providing direction on developing guidance, best practices, and other reference material or activities.

IATA and the International Coordinating Council of Aerospace Industries Associations (ICCAIA) put together the **Aircraft Cyber Security 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 2021 IATA published the **Aviation Cyber Security (ACyS) Guidance Material**. This high-level document was developed with IATA Members and provides operators with considerations on adopting a minimal cyber security posture to organization June 2022.
and aircraft operations. Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation, another publication, covers all legal instruments, regional standards and provisions, recommended practices, industry standards, guidance, and best practices that the industry faces in terms of cyber security.

International Engagement and Collaboration

The Aviation Cyber Security Strategic Partnership package was launched in 2021, to facilitate exchanges and collaboration among cyber security organizations and subject matter experts (SMEs). Moreover, to support the airline industry in the area of aviation cyber security, IATA signed an MoU with the Consortium for Research and Innovation in Aerospace in Quebec (CRIAQ), Israeli National Cyber Directorate (INCD), and EUROCONTROL.

IATA is also holding its 2nd Workshop of the 3 Cyber Threat eXchange 3CTX Open Forum, 21-23 June 2022, in Montreal. In this invitation only forum, airlines will exchange and share the challenges of industry stakeholders including, ANSPs, OEMs and systems providers, academia and researchers as well as the broader cyber security community. The overall goal is 2-fold, one, to bring Cyber Security experts closer to the civil aviation, second, is to increase the respective knowledge of the civil aviation ecosystem.

IATA is involved in the aviation cyber security work at ICAO, including the Secretariat Study Group on Cybersecurity (SSGC), whose work concluded in April 2022. IATA will be part of the new Cybersecurity Panel, CYBERP, which should continue the work of the different subgroups of the SSGC, currently contributing to the ICAO Cybersecurity Glossary or Terminology. 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 cyber security, as well as a study on the international legal instruments. Another area of involvement falls under the ICAO Trust Framework Study Group (TFSG), where IATA supports the revision of the SWIM / PANS-IM information security requirements and is part of different sub-groups.

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. Currently, IATA supports the development of the Acceptable Means of Compliance (AMC) and Guidance Material to support this rule. Moreover, IATA is also part of the EUROCAE WG-72, supporting the development of the standard document ED-206 Guidance on Information Security Event Management.

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