Aviation Cyber Security
Fact Sheet

From the corporate side of the airline to the aircraft 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. As the global pandemic puts pressure on the industry, this trend is expected to accelerate as airlines retire older, more fuel- and maintenance-intensive aircraft. 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. From sensors to artificial intelligence and highly automated systems, the industry is including more and more common off-the-shelf devices and applications to connect to the aircraft. 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. From preemptive maintenance to automation, passed by mobile devices such as tablets in the cockpit, these new technologies significantly enhance aircraft capabilities while simplifying many routine tasks.

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. This work is guided by the Security Advisory Council (SAC) and Digital Transformation Advisory Council (DTAC). Together they advise IATA towards answering the cyber security challenges faced by IATA and the airline industry.

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.
- **Communication and collaboration**: Creating stronger relationships among players in the aviation industry and with 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 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.

With the advent of Covid-19, IATA and relevant stakeholders put together a series of cyber security recommendations, regarding prolonged aircraft storage and the restart, which was presented as an information Paper at the 8th ICAO Secretariat Study Group in Cybersecurity SSGC meeting. Those recommendations are referenced in the latest edition of Guidance for Managing Aircraft Airworthiness for Operations During and Post Pandemic.
Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation 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.

IATA and ICCAIA are putting together a Restricted Forum, where 10 participants of each organization, will work together in order for airlines, to better understand the risks associated with the introduction of new technologies, as well as for the OEMs/Suppliers, and Design Approval Holders DAH, to better understand the struggles and challenges the airlines are facing. This forum should enhance the collaboration between parties and enhance the cyber security posture of the airlines.

Together with the DTAC, IATA is putting together a CISO Forum that will support the cyber security challenges, the corporate side of the airlines are facing.

In September 2019, IATA presented to the 40th ICAO Assembly the Information Paper A40-WP/395 Aviation Cyber Security – Moving Forwards explaining the need for a coordinated, proactive, and tangible progress on gaining visibility to and managing aviation cyber security risks. Through this paper, IATA also gave its support to the creation of the ICAO Cyber Security Strategy.

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

Source: P. Cooper, Aviation Cybersecurity; Atlantic Council (2017).

1 https://www.icao.int/Meetings/A40/Documents/WP/wp_395_en.pdf
2 https://www.icao.int/Meetings/A40/Documents/WP/wp_028_en.pdf