Aviation Cyber Security

Background

IATA has successfully represented the airline industry since 1945. In that time, there have been numerous challenges stretching across security, safety, and commercial. In the current age of intensified digitization and connectivity, the airline industry is now dealing with a complex and critical challenge, namely aviation cyber security.

Aviation cyber security may be considered as the convergence of people, processes, and technology that come together to protect civil aviation organizations, operations, and passengers from digital attacks. Therefore, the aviation cyber security pertaining to the overall environment that interconnects and interacts throughout the entire lifecycle of the aircraft (i.e., design, certifications, operations, and maintenance) is IATA's focus. This focus interlinks with the operations of the following stakeholders, but not limited to, airlines, airport operators, air navigation service providers, original equipment manufacturers, regulators, etc.

Aviation cyber security is a crucial priority for the airlines and the broader industry. The increased level of digitization and connectivity, particularly, helps to transform approaches to customer experiences, aviation operations, delivery by service providers, and regulatory framework. However, this not only brings many advantages, but also risks associated with the challenge of finding and managing cyber vulnerabilities across complex, international operations from airports, aircraft operators, air navigation service providers, and supply chain. This complexity makes the aviation sector globally interdependent and vulnerable to hidden risks and ever-increasing threats. It should be expected that, like today, adversaries will continue their efforts to exploit vulnerabilities in systems for financial gains, reputational, and aviation disruption. Notwithstanding this, the threat of cyber-attacks linked to terrorism in the aviation industry is assessed as low. Continuous improvement and evolving measures are required to strategically safeguard the industry against new types of threats as the surface of attacks is expanding rapidly.

IATA's Role

It can be challenging for the airline industry to drive a positive cyber security change, increase transparency, and make appropriate, risk-based decisions on cyber security. As an informed advocate for cyber security improvements across all aspects of the industry, IATA can advise on and set relevant industry standards and represent its members in regional and international forums.

With IATA in a global leadership role, it will be in a strong position to drive the harmonization of aviation cyber security regulations, approaches, and risk management. For its members and the wider industry, this will lead to reduced complexity, better awareness of risk, efficiencies, and increased international resilience.

IATA's Position and Way Forward

Internal Governance and Structure

As part of the formal IATA governance, the Security Advisory Council (SAC) advises and guides IATA towards answering the aviation cyber security challenges and opportunities faced by IATA and its airline members. The SAC identifies pain points, endorses the development of SARPs as well as speaks with one voice to improve cyber security posture, and reduce complexity. Furthermore, the aviation cyber security cross-cutting issues related to, inter alia, safety, privacy of data, the Passenger Standards Conference (PSC), etc., are collaboratively addressed with the Safety, Flight and Ground Operations Advisory Council (SFGOAC) and the Digital Transformation Advisory Council (DTAC).

Aviation Cyber Security Action

Moving forwards, to support the industry in addressing ever-evolving landscape, IATA is developing an industry-wide Aviation Cyber Security Strategy to coordinate and calibrate, through advocacy, standards, and services, the most appropriate level of holistic cyber protection for the industry. The work to address provisions of the strategy, as well as a high-level work plan, will be carried out by the Cyber Management Working Group (CMWG) in order to address all the cyber security activities in support of the IATA airline members. A proposal for the creation of the CMWG is under review. Once established, the group will sit under the SAC governance and will be jointly led with the DTAC.

Furthermore, through the work of the Aircraft Cyber Security Task Force (ACSTF), and new focused and agile communities of trust, IATA addresses airline concerns related to understanding and managing cyber threats and risks concerning the safety-of-flight. Another critical component of this strategy is the Aviation Cyber Security Roundtable (ACSR), an annual gathering of different stakeholders, exchanging about the aviation cyber security landscape, which helps shape the vision of IATA's cyber security elements.

Next Steps

In order to address this complex and critical challenge, IATA will ensure that appropriate partnerships are established that will enable the Aviation Cyber Security Strategy to be delivered. Thus, IATA will engage with its members, industry leaders, and stakeholders to develop and subsequently communicate the IATA's role in global aviation cyber security. This includes the establishment of a wider collaboration with the original equipment manufacturers (OEMs), regional organizations, and communities as well as academia.

By advocating for positive cyber security change and the needs of airlines across the globe, IATA, if appropriate, will highlight poor practice, challenge unreasonable cyber security practices and strive for sensible regulations, standards, and best practices through influence and engagement with the IATA airline members and industry stakeholders. This will help in a review and implementation process of possible aviation cyber security relevant standards, and recommended practices via the IOSA Standards Manual (ISM) to be considered in view of the IATA Operational Safety Audit (IOSA), to enable greater insight and guidance for potential improvements to the systems.

Furthermore, considering the impact of the global epidemic of COVID-19, IATA will ensure to help its members with the solutions for the post-COVID-19 aviation cyber security posture in order to support the safe and secure restart of the industry operations.

Collaboration with ICAO

To address cyber threats and ensure the civil aviation industry is resilient to cyber-attacks as well as remains safe and trusted at a global level, in 2019, the ICAO Aviation Cybersecurity Strategy1 was endorsed. Following the outcomes of the ICAO 40th Assembly Session, the need for taking further action to counter cyber threats by states and industry was emphasized. Therefore, ICAO was called to develop a Cyber Security Action Plan supporting the process of strategy adoption.

IATA strongly supports the position of ICAO as the most appropriate organization to drive coherent global dialogue and action on ACS. IATA is closely collaborating with the ICAO Secretariat Study Group on Cybersecurity (SSGC) and Trust Framework Study Group (TFSG) to contribute to the development of the action plan for the strategy implementation.

Conclusion

On aviation cyber security, IATA, along with the airline industry and other air transport industry stakeholders, face complex, critical challenges that will shape the resilience of the aviation industry.

The critical, complex nature of aviation cyber security challenges and the associated inherent risks directly aligns with the IATA principles and how it uniquely supports its members. Only by increasing understanding of the aviation cyber security challenge facing the air transport industry, the changes can be effected. Through leadership and acting now, IATA can positively shape the nature of 'how' the industry responds to the aviation cyber security challenge.

[1] ICAO, Aviation Cybersecurity Strategy, October 2019.