Position Paper on

Cybersecurity

THE ISSUE AND POSITION

As one of the most complex and integrated systems of information and communications technology (ICT) in the world, the global aviation system is a potential target for a large-scale cyber-attack, or for attack on one or some of its elements.

The airline industry operations are highly dependent on the reliable functioning of critical computer systems infrastructures (e.g. flight management systems, electronic flight bag, e-enablement of aircraft and extending to air traffic management). This dependence is increasing and so is the concern of vulnerabilities towards cyber-attacks.

With aviation industry gaining operational efficiency through the introduction of computer systems, and their integration to optimize the management of their networks, the number of software systems, connectivity and entry points is raising constantly. Systems and processes are becoming more convenient, efficient and integrated, but consequently increasingly vulnerable to cyber threats.

The potential consequences of a successful act of unlawful interference perpetrated against the aircraft operations through air traffic management systems, flight-safety essential aircraft system or core security airport systems may result in imminent life risks to passengers, airlines crew and people in the air and on the ground.

IATA believes that cyber threats to the security of operations (with the potential to result in an act of unlawful interference) are real and its likelihood increasing. It depends on the capabilities and the intentions of potential perpetrators.

A strong involvement and collaboration between the organizations and entities in the value chain is required to maintain a coherent and sustainable cyber resilience strategy for the global civil aviation industry and for it to manage effectively the risk.

IATA recognizes the need to raise awareness of the subject within the airline’s community and with their value chain partners (air traffic management, aircraft manufacturers and maintenance entities, airports, service providers, governments and others) with particular focus on preventing acts of unlawful interference which might be committed with the use of cyber means.

IATA believes in threat-based, risk-managed and outcome-focused frameworks balanced against industry capabilities and sustainability instead of the adoption of prescriptive measures.

BACKGROUND INFORMATION

Today many organizations, industry and government agencies are involved in assessing the cyber threats and risks as well as developing protective measures and solutions for the integrated systems of information and communications technology used by the aviation sector.

ECAC as of 2010 worked on new recommendations and started the development of the guidance material on cyber.

CANSO representing air navigation services organizations published its Cyber Security and Risk Assessment Guide in June 2014 as practical guidance for improving cybersecurity awareness across the ATM industry.

IFALPA representing airline pilots has developed an action plan aim at addressing the cyber threat. It proposes actions to be undertaken by various stakeholders.

IATA in 2013 developed its three-pronged strategy for cyber covering Risk Management, Advocacy, Reporting and Communication and has been assisting member airlines in developing, implementing and enhancing their cyber security programs through the testing on the Cybersecurity Toolkit and increasing awareness through outreach campaigns around the globe.

ACI Europe developed a briefing paper in March 2014 (Cyber Security: Potential Impact on EU Airports) where it highlighted an increasing exposure of airports for cyber threats, including those related to acts of unlawful interference. It proposed also a number of actions to be considered by airports to tackle the issue.

Proposed solution

IATA to:

- Continually update its position on cybersecurity to represent the interests of its members
- Develop new venues for cooperation with stakeholders and entities to work on cyber mitigation measures for the aviation industry
- Assist its members in maintaining and sharing best practices in relation to cyber mitigation and resilience and business continuity
- Support continuous monitoring and assessment of the potential risks, particularly in relation to the prevention of unlawful interference against aircraft.
- Proactively advocate to governments and industry regulators smarter regulations and the prevention of excessive or prescriptive legal frameworks that would challenge industry capabilities to overcome the cyber threat