



THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE A

Agenda Item 5: Emerging issues

5.4: Cyber resilience

AIRPORT PREPAREDNESS ON CYBER RESILIENCE

(Presented by Airports Council International (ACI))

EXECUTIVE SUMMARY

This paper presents ACI's airport-specific initiatives on resilience to cyber security attack, supporting the working papers presented by the ICAO Secretariat on cyber resilience.

Action: The Conference is invited to:

- a) note the work being undertaken by ACI and its members and
- b) agree to the recommendations in paragraph 4.3.

1. INTRODUCTION

1.1 Airport systems are increasingly connected with the systems of aircraft operators, air navigation service providers (ANSPs) and ground handling service providers, and all such systems are mutually dependent for the exchange of digital information. This information exchange is key to addressing airport capacity constraints and improving efficiency, including through airport collaborative decision making (A-CDM) and ultimately total airport management (TAM). Cyber related threats and incidents can affect these systems, hence ACI fully supports the Secretariat's working paper on cyber resilience (AN-Conf/13-WP/27 refers) and encourages airports to address this issue through implementation of appropriate cyber security policies and frameworks.

2. DISCUSSION

2.1 Airports are rapidly introducing new digital assets and related processes to facilitate automation, infrastructure-to-passenger interaction and vice-versa. This digital transformation, automation and increasing reliance on data brings with it the challenge of keeping systems and information secure.

2.2 It is recognised that airports, as with other stakeholders, need to identify existing and new cyber security threats, increase their awareness of security issues, conduct robust risk assessments on their systems and networks and improve the security of their infrastructure through the implementation of best practices.

2.3 A successful cyber-attack can cause disruption to airport operations, loss of proprietary information and other strategic assets and, affect airport business reputation and stakeholder trust. Effects of cyber-attacks on businesses can be financial, reputational and legal. Because of the interconnected nature of the air transport network, an attack on one system or one airport can severely affect the operation of the entire system.

2.4 The maturity of airports in terms of information technology varies widely, depending on the size of operation, the management of the airport and the location. Regardless of the level of sophistication, best practices in terms of network separation, protective measures such as firewalls, robust monitoring processes and solid contingency plans are all applicable.

3. ACI INITIATIVES

3.1 Given the importance of this topic, the World Annual General Assembly of ACI passed a resolution in June 2018 to reaffirm the commitment of airports to addressing cyber security (Appendix). ACI has already commenced the development of a range of tools and guidance to assist airports to manage their cyber security implementation.

- (a) **Self-assessment tool.** ACI's cyber security self- assessment tool provides airport stakeholders with a snapshot of their information security management strengths and weaknesses. Based on International Standards (ISO 27002), this user-friendly tool provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS). It also provides the ability for airports to benchmark themselves against others.
- (b) **Guidance handbooks.** Two ACI handbooks are currently under development. The first will provide guidance to executive level management on the importance of cyber security, the potential threats, impacts and actions that should be undertaken. The second document is designed for middle management to help airports to understand best practices for addressing cyber security threats, from the management level through to technical strategies. These handbooks will also help airports that already have an established cyber security policy, to validate or improve their systems.
- (c) **Training courses.** ACI has a partnership agreement with Munich Airport's Information Security Hub for collaboration on a set of technical training courses on cyber security. A further set of courses under development, designed to reach both senior management in airports, and those responsible for business systems who require more in-depth knowledge of cyber security strategies.
- (d) **Assistance.** ACI has a team of experts ready to help airports understand their cyber security risk, improve their protective measures and build resilience to cyber-attack.

4. FUTURE INITIATIVES

4.1 ACI strongly supports collaboration with States and other stakeholders to ensure a practical, coordinated effort in addressing cyber security threats. ACI and its members play an active role in the work of ICAO at the global level in cyber security, including contributions to existing guidance materials, as rapporteur for the Working Group on Aerodromes under the Secretariat Study Group on Cyber Security, and through participation in other groups.

4.2 ACI supports the need for a globally harmonized aviation trust framework for data exchange that affects safety critical systems, and encourages the work described in AN-Conf/13-WP/27. It will be important in this work, and in other projects being undertaken, that a risk-based approach is taken to prioritization of efforts. The scope of cyber security is enormous, and there is a need to consider likelihood of attack, vulnerability of systems and likely impacts of attacks. For this reason, ACI believes that the work of ICAO should focus on safety-critical systems and those that could affect the integrity of the air transport network.

4.3 At the industry level, ACI will continue its work to ensure that airports implement best practices for all systems, understanding financial and operational impacts of attacks across their entire IT infrastructure.

Recommendation 5.4/x

The Conference is invited to:

- a) note the provided information on ACI initiatives that should protect low risk/internal systems;
- b) request ICAO to support the development of a trust framework for safety-critical systems; and
- c) recommend States and ICAO work with industry to ensure that practical, efficient, flexible and effective cyber security regulations and measures are implemented.

— — — — —



APPENDIX

AN EFFECTIVE APPROACH TO CYBER SECURITY

The Twenty-eighth ACI World General Assembly:

Recognizing that there are a growing number of cyber-attacks around the world;

Recognizing that cyber-attacks are becoming more sophisticated;

Recognizing the financial, operational and safety critical impact that cyber-attacks may have on airports and the aviation system;

Noting that ICAO has prioritised cyber security and is currently working to define and propose a framework for the Aviation Industry;

Noting that there are many different regional and national approaches to cyber security at the regulatory level; and

Noting that airports have varying degrees of complexity in IT systems and different frameworks for cyber security; therefore.

The General Assembly resolves to:

- a) support the establishment of an ACI policy to address cyber threats at airports;
- b) support the principle of a flexible, outcome focused approach to regulation that takes into account the measures implemented by industry;
- c) support a practical and effective approach to cyber security regulation through close cooperation with ICAO and national regulators;
- d) encourage the exchange of information between airports, national regulators, intelligence agencies and other industry stakeholders to ensure that there is a common understanding of cyber security risk and threat information;
- e) request that ACI coordinates activities with ICAO to ensure that airports interests are represented at the global level;
- f) encourage ACI to develop cyber security best practices and tools that offer an approach to identifying threats, prioritizing risks and implementing countermeasures that can help airports prevent, respond to and recover from attacks, building on existing frameworks;
- g) urge ACI to continue to develop cyber security training courses to provide management level knowledge and understanding, approaches to cyber security management frameworks and technical guidance that can be put into practice; and
- h) encourage ACI to enhance the existing Cyber Security self-assessment tool to help airports identify potential improvements to their cyber security programmes.

— END —