International Civil Aviation Organization

WORKING PAPER

A40-WP/532
EX/228
10/9/19
(Information paper)
English only

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 12: Aviation Security – Policy

AVIATION CYBER SECURITY

(Presented by the State of Qatar)

EXECUTIVE SUMMARY

This information paper describes the State of Qatar's approach to introducing aviation cyber security guidelines and aviation cyber security policy within the National Civil Aviation Security Programme.

Strategic Objectives:	This information paper deals with aviation cyber security.
Financial implications:	No financial implications.
References:	Annex 17 – *Security* ICAO Doc 10118, *Global Aviation Security Plan* (GASeP) ICAO Doc 8973, *Aviation Security Manual* ICAO Doc 10108, *Aviation Security Global Risk Context Statement* (RCS) National Civil Aviation Security Programme (NCASP) for the State of Qatar

1. INTRODUCTION

1.1 The civil aviation sector relies increasingly on the use of data and interconnected technology to streamline facilitation and increase efficiency. Manual processes are being replaced with sophisticated technology across almost every segment of civil aviation. With the increased use of technology and interconnected systems, inherent risks and vulnerabilities are exposed, along with various external threats. Every stakeholder in the aviation system must therefore identify its critical information systems and develop and implement suitable protective measures to mitigate against these vulnerabilities.

1.2 An analysis of the present-day data systems and various other critically important national mechanisms within Qatar has revealed that such systems remain attractive targets that could be exploited by determined experienced attackers. Within Qatar there has not been a cyber-attack specifically targeting aviation related systems, however this might change in the future. Doc 10108, the *Aviation Security Global Risk Context Statement* (RCS) determines that the risk of cyber-attacks in the aviation Industry remains *low*; however, "**potential vulnerabilities have been identified and the risk could well increase as current technological trends continue**." The RCS also confirms that there is some evidence of intent by terrorist organisations to attack aviation targets using cyber-attacks, although their capability to do so remains doubtful. This could possibly change in the near future as they gain expertise in this area.

2. ANNEX 17

2.1 Annex 17, Standard 4.9.1 states: " **Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference**."

2.2 Recommended Practice 4.9.2 states: "**Each Contracting State should ensure that the measures implemented protect, as appropriate, the confidentiality, integrity and availability of the identified critical systems and/or data. The measures should include, inter alia, security by design, supply chain security, network separation, and the protection and/or limitation of any remote access capabilities, as appropriate and in accordance with the risk assessment carried out by its relevant national authorities."**

2.3 Qatar has established an aviation cyber security framework within the National Civil Aviation Security Programme (NCASP) to optimize the use of technology whilst maintaining high cyber security standards.

3. SITUATION

3.1 For the reasons mentioned above, Qatar established a joint aviation cyber security committee which aims at aligning the national cyber framework with the best international practices applied today. The starting point was the introduction into the NCASP of specific cyber security policy requirements and the development and publication of aviation cyber security guidelines for all aviation stakeholders within Qatar. The development of the guidelines incorporated a period of industry engagement. The guidelines help in defining the scope of the aviation cyber security system and also guide relevant stakeholders towards NCASP compliance by identifying the most critical systems within their organizations and implementing appropriate mitigation measures. The joint aviation cyber security committee is currently working on the establishment of a competent department within the Ministry of Transport and Communication (MOTC) to help the QCAA perform oversight and assist from a technical perspective to achieve the best outcome.

3.2 Within the NCASP, the MOTC is the responsible Government agency for securing and enhancing the efficiency of Information and Communications Technology (ICT) in Qatar. The Qatar Computer Emergency Response Team (Q-CERT) was established to comprehensively address and respond to risks that may arise with technology usage and build resilience into the critical information infrastructure of Qatar. Q-CERT's Incident Response Service provides the capability to address and respond to security incidents that may occur as a result of the use of technology. The Qatar Civil Aviation Authority (QCAA), in conjunction with the MOTC and other relevant authorities, is responsible for coordinating the national aviation cyber security strategy for Qatar. The practical implementation of this strategy is the responsibility of all security programme holders and all other persons to whom the NCASP applies.

3.3 The MOTC, in collaboration with the QCAA, has developed a guidance document entitled "Aviation Cyber Security Guidelines" that is designed to help the aviation industry within Qatar in identifying and adopting secure best practices and good cyber hygiene. These guidelines are contained in an Appendix to the NCASP that is available to all stakeholders via the QCAA website. The Aviation Cyber Security Guidelines highlight the key aspects which form the basis of any IT system. These key aspects are:

a) System and network design;
b) System and network security;
c) Communication security;
d) Product security;
e) Software security;
f) Cloud security;
g) Industrial control systems and Internet of Things (IoT);
h) Identity and access management;
i) Cryptography;
j) Media security; and
k) Bring your own device (BYOD).

3.4 All security programme holders and all other persons to whom the NCASP applies are required to ensure that all personnel tasked with securing critical information systems are properly selected, recruited and trained. Cyber security training and awareness are essential elements of an organization's overall aviation cyber security system. All security programme holders and all other

persons to whom the NCASP applies are also required to retain records of their cyber security training or awareness programs and must produce such records when requested for auditing and inspection purposes.

3.5 All security programme holders and all other persons to whom the NCASP applies are required to report immediately the occurrence of any cyber security threat or incident in accordance with relevant sections of the NCASP.

3.6 The QCAA, jointly with the MOTC, conducted a comprehensive survey and assessment of the systems within Qatar and also consulted all relevant stakeholders to capture all the relevant critical elements within Qatar's civil aviation system. In addition, the QCAA, with support from the MOTC, conducted a limited penetration testing which was focused on some of the web-based secure services. The outcomes were very positive and there were many lessons learned as well. The approach and methodology used for the development of the guidelines will be presented at the upcoming ICAO Cyber Security and Resilience Symposium in Amman, Jordan, 15-17 October 2019.

4. CONCLUSIONS

4.1 The joint aviation cyber security committee will continue its efforts in developing the aviation cyber security strategy in Qatar through collaboration with stakeholders and with other ICAO Member States. Also, the committee is preparing a list of future activities and exercises such as inspections and penetration tests of more critical systems which are planned to take place in 2020.

4.2 The Assembly is invited to note the contents of this IP.

— END —