RAAC/14-WP/16
06/10/15

International Civil Aviation Organization
ICAO South American Regional Office
Fourteenth Meeting of the Civil Aviation Authorities of the SAM Region (RAAC/14)
(Santiago, Chile, 27, 28 and 30 October 2015)

Agenda Item 3: **Review of results obtained in the SAM Region on security matters**

CYBER SECURITY AND RISK ASSESSMENT GUIDE

(Presented by CANSO)

SUMMARY

As ATM moves towards open standards and systems, ANSPs will need to become more knowledgeable about the threats they face and more flexible and responsive in their actions to counter them. As the cyber threat is continually evolving and becoming increasingly sophisticated, ATM must assess the vulnerability of processes and assets to attack, whether from internal or external sources, and put in place the necessary mitigations.

To assist ANSPs, CANSO published its *Cyber Security and Risk Assessment Guide*, which recommends conducting a cyber-risk assessment as a first step to understanding and managing the cybersecurity risks to systems, assets, data and capabilities in ATM.

References:

- ICAO DOC. 9854
- CANSO Cyber Security and Risk Assessment Guide

***ICAO Strategic Objectives*:**	*A - Safety* *D – Economic Development of Air Transport* *E – Environmental Protection*

1. Introduction

1.1 In response to the increasing threat of cyber-attacks on air traffic management (ATM) systems CANSO published its *Cyber Security and Risk Assessment Guide* in June 2014, as practical guidance for improving cybersecurity awareness across the ATM industry. The Guide provides CANSO Members with an introduction to cybersecurity in ATM and includes an overview of the cyber threats and risks and motives of threat actors; some considerations for managing cyber risks; and suggestions for implementing a cybersecurity programme. The appendices further include information on standards; a framework for cybersecurity; and some practical guidance to conducting a cyber-risk assessment – a recommended first step to understanding and managing the cybersecurity risks to systems, assets, data and capabilities in ATM.

2. **Discussion**

2.1 Historically, information and communications technology (ICT) in ATM has been using point-to-point links to exchange information between bespoke systems hosted within an ANSP. These solutions have worked, but are expensive with long development times and are generally inflexible. This is changing with the adoption of international (IT) networking and architectural standards as well as the use of commercial off-the-shelf (COTS) software, hardware and services. ATM modernisation programmes such as SESAR, NextGen and Japan's Collaborative Actions for Renovation of Air Traffic Systems (CARATS) have all been designed with this in mind.

2.2 As ATM moves towards open standards and systems, ANSPs will need to become more knowledgeable about the threats they face and more flexible and responsive in their actions to counter them. The cyber threat is continually evolving and becoming increasingly sophisticated. The dissemination of expertise from expert virus writers is accelerating and is distributed through toolkits that can be used by anyone. For example, once Stuxnet[1] was identified it was rapidly adopted and altered at code level and redistributed by top-level virus writers. It was then incorporated into cybercriminal tool kits and sold over the "darknet" – private networks where connections are made only between trusted peers. The cyber world is of increasing interest to criminals who are creating a professional standard and geographically distributed supply chain to conduct cyber warfare. The potential of a terrorist cyber-attack against aviation utilising the ATM system is also very real.

2.3 ATM must therefore tackle the cyber threat by assessing the vulnerability of processes and assets to attack, whether these involve staff or outside parties. The wide range of potential cyber threats and the integrated nature of modern ATM demands a holistic approach and the involvement of all ATM stakeholders. Importantly, risk assessments of ATM systems should take account not only of terrorist-related attacks, but also include attacks perpetrated by hackers who wish to gain access to systems and cause disruption, or attacks carried out for espionage or commercial purposes by State actors. These can be equally disruptive and compromise the safety, security and integrity of the aviation system.

2.4 To assist ANSPs, CANSO published its *Cyber Security and Risk Assessment Guide* in June 2014, which is available at https://www.canso.org/canso-cyber-security-and-risk-assessment-guide. It is meant to provide ANSPs with an introduction to cybersecurity in ATM and includes an overview of the cyber threats and risks and motives of threat actors; some considerations for managing cyber risks; and suggestions for implementing a cybersecurity programme. Among the conclusions in the *Cyber Security and Risk Assessment Guide* is that cybersecurity must be considered as part of ATM security and, more generally, of overall aviation security, in order to fulfil societal expectations of safety and security of the aviation system.

2.5 The *Cyber Security and Risk Assessment Guide* recommends conducting a cyber-risk assessment as a first step to understanding and managing the cybersecurity risks to systems, assets, data and capabilities in ATM.

[1] Stuxnet is a computer worm that was discovered in June 2010, designed to attack industrial programmable logic controllers (PLCs). It reportedly ruined almost one-fifth of Iran's nuclear centrifuges.

3. Suggested action

3.1 The Meeting is invited to:

a) Take note of the information presented in this working paper; and
b) Encourage the use by ATM organisations of the CANSO Cyber Security and Risk Assessment Guide, and the international standards and industry best practices that exist for cybersecurity.

- END -