International Civil Aviation Organization

A40-WP/295
TE/119
1/8/19

WORKING PAPER

ASSEMBLY — 40TH SESSION

TECHNICAL COMMISSION

Agenda Item 30: Other issues to be considered by the Technical Commission

THE APPLICATION OF STATE CYBER-SECURITY CONTROLS TO AVIATION

(Presented by New Zealand)

EXECUTIVE SUMMARY

This paper discusses the development of ICAO aviation cyber-security frameworks in the context of existing non-sector-specific cyber-security controls used by States. It proposes that ICAO should focus its efforts on developing robust & agreed principles from which States can approach cyber security issues.

Action: The Assembly is invited to agree to:

a) note that the implementation of global harmonised and overly prescriptive aviation cyber-security standards may conflict with States' national cyber-security frameworks and constrain the ability of states to comply with ICAO SARPs,
b) encourage ICAO to focus on the development of principle-based guidance on aviation sector cyber-security to assist States with integrating aviation into national frameworks, taking into account established information security standards such as the ISO 27000 series; and
c) encourage ICAO to provide guidance on the purpose and application of the trust framework.

Strategic Objectives:	This working paper relates to Strategic Objectives: Security and Facilitation, and Safety
Financial implications:	None
References:	AN-Conf/13-WP/270: System-of-Systems Notion of Cybersecurity in Aviation (28/09/2018)

1. INTRODUCTION

1.1 With continued advances in technology and the growing levels of complexity in aviation systems, the safety and security of the global aviation system is becoming increasingly reliant on effective cyber-security controls.

1.2 The need for effective cyber-security controls is common across a wide range of different sectors and is by no means unique to aviation. Without effective cyber-security, organisations will struggle to deliver digital products and services in a way that retains the trust and confidence of their customers and stakeholders.

1.3 States have a role to play to ensure nationally significant organisations and sectors to achieve consistently high levels of cyber-security. The approach taken will vary from State to State in response to differing threats, capabilities and national security interests.

1.4 Although the type of security controls put in place by individual organisations will generally be tailored to their needs and capabilities, and those of the sector in which they operate, national security interests will impose overarching requirements. A State's national interest will always take precedence over that of an individual sector or organisation.

1.5 Global aviation is highly reliant on the safe and secure digital transmission of information between members of the aviation community, including between states. Paper AN-Conf/13-WP/270 presented at the Thirteenth Air Navigation Conference introduced the concept of a "System of Systems" approach to cyber-security. This approach recognises that the overall aviation system is made up of a number of sub-systems operated by a range of stakeholders, and that these need to be considered holistically to achieve a secure operating environment.

1.6 The ICAO Trust Framework has been developed to enable the establishment of trusted communication links between stakeholders. The Framework encompasses the following principles:

1.6.1 Interoperability between all stakeholders is assured through a common trust framework and architecture for seamless and efficient messaging services on a global scale.

1.6.2 Resiliency of the communications is maximized by utilizing design concepts that limit the threat surface. This includes compartmentalization of the network and the applications, as well as layering of protections in the infrastructure and limiting the number of systems participating.

1.6.3 Strong identification, authentication, authorization, integrity, and confidentiality.

1.7 Although the concept of the trust framework has value, there is a lack of clarity around its purpose and potential application. Further development of the framework will require careful consideration of states' national security interests to ensure that its role is clearly defined.

2. DISCUSSION

2.1 A State's national interests impose constraints on the nature of the cyber-security frameworks that can be implemented by individual sectors and organisations. Where there are State regulatory requirements and standards for the security of information, these will take precedence over sector and organisation-specific standards.

2.2 As such, a State's ability to comply with prescriptive ICAO SARPs for aviation cyber-security is likely to be constrained by its own national security frameworks. The extent of this constraint will vary significantly from State to State and the degree of prescription in the SARPs themselves.

2.3 Similarly, it is unlikely that a highly prescriptive and highly standardised approach would effectively regulate an area where technology and the threat environment are both evolving at a rapid pace. Overly prescriptive global requirements may hinder a State's ability to respond to change, and may not be equally appropriate for differing types of operation.

2.4 Despite the differing cyber-security needs of individual States, and the issues with imposing highly prescriptive international requirements, there is a need for a consistent and agreed set of principles to govern the secure transfer of information between stakeholders.

2.5 To support the implementation of these principles, ICAO guidance material should be developed with a focus on assisting states to support aviation cyber-security as an integral part of national frameworks. To achieve this, a performance or principle-based approach is likely to be most effective.

2.6 By adopting a principle-based approach, ICAO guidance could be adapted by individual states in a way that enables a global trust framework to be implemented in line with national requirements. Existing principle-based information security standards, such as the ISO 27000 series, provide a basis for such guidance. There are four focus areas that would ideally be addressed:

2.6.1 **Governance**: Promoting cyber security at a senior leadership level to protect an organisation's most important digital assets. Boards and executives are ultimately responsible for the outcomes of any cyber incident, including the impact on stakeholder and customer confidence.

2.6.2 **Investment**: Investing in cyber security to minimise risk and maximise returns. Agreement at a governance level on the organisation's risk appetite and identification of key assets are critical first steps to ensure investment is directed and balanced appropriately.

2.6.3 **Readiness**: Preparing the organisation to detect, respond, and recover from a cyber-security incident. It is a matter of 'when' not 'if' an organisation will experience a cyber-security incident. Readiness for an incident enables organisations to reduce the overall cyber security risk through prompt and effective recovery.

2.6.4 **Supply Chain**: Maintaining oversight and awareness of the cyber security risks in an organisation's supply chain. This area is particularly important in the aviation sector as there are often lengthy supply chains involved in the delivery of equipment and services. This includes the technical component of systems design, and the human factor aspect of process design.

2.7 Well-formulated performance-based guidance, based on established information security standards, would be of value to individual organisations within the aviation sector, and would encourage a consistent approach covering the critical elements of effective cyber-security controls.

2.8 The development of such guidance should also consider where there is a need for certain minimum controls, and how these should be approached taking into account the frameworks applied by different States.

2.9 The development of the ICAO trust framework provides an opportunity to set out protocols for the interchange of information between stakeholders, but further clarification as to its purpose and application is needed.

2.10 The development of the trust framework should be considered in conjunction with the cyber-security frameworks implemented by stakeholders. The security of data exchange is only as good as the security of the data source, and this is dependent on effective controls being adopted by organisations and States.

— END —