International Civil Aviation Organization

AN-Conf/13-WP/171
28/9/18
English only

WORKING PAPER

THIRTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 9 to 19 October 2018

COMMITTEE A

Agenda Item 5: Emerging issues
5.4: Cyber resilience

CYBER RESILIENCE IN THE SWIM CONCEPT

(Presented by the Civil Air Navigation Services Organisation (CANSO))

EXECUTIVE SUMMARY

This paper presents the view of CANSO how to protect the SWIM concept against future cyber threats.

Action: The Conference is invited to:

a) advise ICAO to clearly define the commitment in the governance of the cyber protection of aviation by including it in the project phase (security by design) and by imposing a clear vision in the deployment and operation phases (security through lifecycle). This has to be included in all relevant ICAO Standards and Recommended Practices (SARPs) contained in the relevant Annexes such as Annex 17 — *Security — Safeguarding International Civil Aviation against Acts of Unlawful Interference*, Annex 19 — *Safety Management* and others where appropriate;
b) confirm that States and operators need to promote a security culture for all actors in aviation including publishers, internal/external users and international users;
c) advise ICAO to create guidelines for States that will define a clear matrix of roles and responsibilities to ensure that the protection layer is proactively managed and even weak signals of potential acts of unlawful interference can be captured, analysed and managed; and
d) advise States on the need to create contingency plans based on a local and international risk and threat approach to mitigate disruptions within the system as a result of cyber-attacks or cyber failures.

1. INTRODUCTION

1.1 System-wide information management (SWIM) is about dynamic, effective and timely information management that will be constantly available to aviation stakeholders. These requirements refer not only to efficient, resilient and interoperable systems, but also to efficient organisations, appropriate common legal frameworks and effective governance. This requires new skills and measurement, including defined security targets.

1.2 This evolution towards SWIM, requires the implementation and consideration of "duty of care", referring to the primary objectives of aviation security as envisaged in Annex 17 — *Security — Safeguarding International Civil Aviation against Acts of Unlawful* Interference to the Convention on

International Civil Aviation (Doc 7300). The complexity of information security requires the implementation of principles, "security by design" and "security through the life cycle". Coincidently, a change of perspective from the static "compliance" to the need to actively ensure the duty of care through proactive diligence must occur. This day-by-day approach is aimed at preserving and protecting the sensitive public interests in the civil aviation.

1.3 It is essential to establish a methodological approach on information security to ensure the active protection of SWIM components (data and systems). These components must be protected from interference and access must be limited to authorised personnel. Related measures have to be risk-based, sustainable, appropriate, and based on existing standards and best practices. This due diligence ensures compliance with regulations and the primary objective of aviation security, as envisaged in the context of the Convention on International Civil Aviation and its Annexes and Technical Instructions.

1.4 Information security is a matter of technology and human interface including; training, awareness, insider threat mitigation and positive behaviour recognition, all framed in an appropriate set of rules and procedures. This is key for successful actions to continuously improve SWIM effectiveness.

2. BACKGROUND

2.1 SWIM is essential for the modern air traffic management (ATM) systems such as NextGen, Single European Sky, CARATS and others, facing new challenges inspired to safety, efficiency and resilience. The fundamental premise of SWIM, requires complete information availability at multiple levels with a plurality of recipients and with a degree of reliability consistent with the expected requirements of safety, security, affordability and availability. Access to SWIM must be granted only to those authorised on a need-to-know basis.

2.2 The SWIM architecture assumes the existence of a multi-level security process which guarantees "information consumers" and "information providers" the appropriate level of resilience. This resilience is achieved through threat analysis globally considering equipment, processes and personnel.

2.3 This modern concept of aeronautical information must at every stage, consider security as a main requirement. The design and production of the architecture should include the entire life cycle, using a model of adaptive governance, according to the criteria, best practices and principles of international, regional and where required, national regulations.

2.4 According to the *Manual on System-Wide Information Management (SWIM)* Concept (Doc 10039), states that "Key to the philosophy adopted within the operational concept is the notion of global information utilization, management and interchange. This philosophy is supported in large part by evolution to a holistic, cooperative and collaborative decision-making environment". Security is a critical factor within this system. For this reason, the global SWIM concept encompasses aspects as, authentication, authorisation, encryption, intrusion detection, security policies, etc.

2.5 Balancing availability, interoperability and information security requirements is the challenge. This stresses the complexity, in terms of architecture (multiple layers: SWIM-enabled applications, information-exchange services, information-exchange models, SWIM infrastructure and related interfaces, network connectivity) and management which must not be impaired by fragmented legal framework and policies.

2.6 Defense against hackers is very complex. The hackers, especially those that are sponsored, have no concerns for processes and procedures; these people appear to have a strong capacity,

with determination and an abundance of resources. The digital evolution of aviation urges States and industry to improve their cybersecurity strategies, allocating appropriate effort and resources. CANSO appreciates the evolution of the current legal framework for the information security domain. The approval of Amendment 16 to Annex 17, Standard 4.9.1. and the rephrased Recommended Practice 4.9.2 is a step forward.

2.7 SWIM requires:

a) a clear definition of the commitment in the governance by including security in the project phase (security by design) and by imposing a clear vision in the deployment and operation phases (security through lifecycle);

b) the propagation of the security culture within all aviation stake holders;

c) the need to consider security ramifications in the whole supply chain, with a special focus on human-related issues and opportunities;

d) creating a clear matrix of roles and responsibilities to ensure the protection layer is proactively managed and robust enough that signals of potential acts of unlawful interference can be captured, analysed and managed; and

e) the organisation of a sound continuity framework, including contingency plans for the SWIM priority services, in case of events that can result in significand degradation or interruption of services.

2.8 Cybersecurity has a direct impact across the entire aviation industry. The nature of this threat requires a new approach in terms of actions, learning from the safety approach taking into account the similarities and differences.

— The risk assessment methodology suffers from the uncertainty of the hostile actors' intent and capability measurement and its outcomes are mostly qualitative and subjective.

— Security management is not only a matter of understanding threats but also realising how internal vulnerabilities could be exploited, not only those related to hardware and software, but also human weaknesses. In this field, the emerging capability of antagonists should be better investigated.

— The new aviation ecosystem requires the consideration of some impairing factors, such as the respect of the right of sovereignty, including the consideration of the need for a new public-private cooperation model which comprises a fast and reliable threat intelligence information dissemination and coordinated actions.

— A real time adaptive response in terms of counter measures and remediation process in a very reliable, efficient and timely manner.

2.9 The SWIM operational concept requires a solid security governance scheme with a clear view on scope, strategies, actions, trust and efficiency measurement. This extends to the whole context of the SWIM environment, including external services providers.

2.10 The users (air navigation services provider (ANSPs), airport operators, airlines, general aviation, military and other government entities, aviation partners and others) should coordinate to create a realistic approach to the standardisation process. They should use the existing standards and best practices commonly agreed in IT aimed at:

a) making security sustainable, risk-based and commonly agreed and supported by a clear commitment;

b) defining a methodology to avoid useless effort, to drive investment and operational expenses both in programme management and in operations;

c) providing common agreed metrics to preserve fair competition; and

d) setting boundaries for accountability.

3. CONCLUSION

3.1 The Conference is invited to agree to the actions in the executive summary.

— END —