International Civil Aviation Organization

WORKING PAPER

A40-WP/395[1]
EX/161
30/7/19
(Information Paper)

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 12: Aviation Security — Policy

AVIATION CYBER SECURITY – MOVING FORWARDS

(Presented by the International Air Transport Association)

EXECUTIVE SUMMARY

The paper presents the International Air Transport Association (IATA) views on the need for co-ordinated, proactive and tangible progress on gaining visibility to and managing aviation cyber security risk.

Strategic Objectives:	This information paper relates to Strategic Objective: Security
Financial implications:	None
References:	

1. INTRODUCTION

1.1 Aviation cyber security (cyber security that pertains to maintaining safe, secure and resilient flight operations), remains a key priority for the sector. Increased digitization and connectivity is helping transform the service available to customers as well as improving everything from efficiency to reliability for regulated operators. But this transformation does not just bring opportunity to the aviation sector, it brings potential opportunity to those who would wish it harm. At a foundational level, the aviation sector is arguably better off than many sectors due to its focus on safety culture, visibility of risk and design and training for redundancy or failure. But service and system complexity and interdependence, often internationally, is potentially impacting the ability to understand and manage cyber security risk.

1.2 IATA strongly supports the position of ICAO as the most appropriate organization to drive coherent global dialogue and action on aviation cyber security. Without clear international leadership on aviation cyber security, we risk fragmentation of global standards, a complex regulatory regime that stifles

[1] English, French, Spanish, Russian, Arabic and Chinese versions provided by the International Air Transport Association.

growth and innovation as well as restricting the ability to assess and manage aviation cyber security risk within and across borders.

1.3 The production of the ICAO Aviation Cyber Security Strategy is a creditable and overdue step that has the full support of IATA. Now, leadership, action and appropriate governance will be required to endorse the Strategy through an amendment of the existing Assembly Resolution A39-19 *Addressing Cybersecurity in Civil Aviation* to incorporate the corresponding reference. Therefore, appropriate resourcing, time and effort alongside all stakeholders, including safety and security, need to be ensured. Moreover, following the hereinbefore, it is important that the ratification by the States of the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* and the *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft*, is encouraged. This collaborative engagement should lead to the development of best practices and guidance materials out of which IATA, in principle, supports the generation of cyber security related SARPs and their subsequent implementation and oversight.

1.4 More broadly, in our endeavors to secure the industry, we cannot forget the lifeblood of our industry which is our passengers and customers. We must ensure that throughout the customer journey, their cyber security, privacy, data and rights are protected. Additionally, ensuring that we as an industry are transparent on these matters, will ensure that we build and secure a trusted relationship with those that support it.

1.5 IATA has been pro-active in raising awareness and stakeholder dialogue about the global challenges of aviation cyber security. IATA has a well-established Aircraft Cyber Security Task Force (ACSTF) which works to increase understanding, drive dialogue and capture best practice across aviation sector stakeholders. The maturity of the ACSTF has created a high trust environment where tangible information sharing on a multitude of related topics have been shared and explored. Additionally, IATA also led a ground-breaking aviation cyber security roundtable in Singapore (April, 2019) with stakeholders representing the full scope of the aviation sector. At this roundtable, stakeholders explored the current challenges facing the aviation industry, what a cyber secure future should look like and how to get there. The findings highlighted that although there is much being done, there remains still much to do.

1.6 Additionally, IATA has begun the process of developing an industry Aviation Cyber Security Strategy along with a road-map to deliver it. The objective of this strategy is to allow IATA on behalf of its members and the wider industry, to bring increased focus to both the challenges and opportunities of the cyber security issues we face, the tangible activity that will make a difference and the collaborations to make it happen.

2. DISCUSSION

2.1 With the current growth figures, by 2037 we could see a doubling of passenger numbers with much of that growth in the Asia pacific region[2]. There are many pressures and risks to this growth and aviation cyber security must be added as one of those risks. The criticality of ensuring the safety, security and resilience of the technology that this growth depends on cannot be underestimated.

2.2 An aviation cyber event does not just risk impact to safety, security, operational services, financial losses or growth. It risks critically impacting passenger confidence and trust in the very service

[2] IATA Press Release, 24 October 2018. IATA Forecast Predicts 8.2 billion Air Travelers in 2037. Available at https://www.iata.org/pressroom/pr/Pages/2018-10-24-02.aspx.

we are delivering. Over many years, the aviation industry has proven that it is resilient to safety or security incidents and is able to rebuild passenger trust through demonstrable measures and engagement. Post an adverse aviation cyber event, rebuilding trust will be an order of magnitude harder than the aviation industry has previously experienced, therefore we need to not only improve cyber security, but also have an open dialogue about the challenge we face and the efforts we are making.

2.3 In our drive for technological advancement, a balance must also be found between promoting efficiencies and service by increased use of connected technologies with the through-life cyber safety, security and resilience of that technology. We can no longer afford to accept any new technology into the aviation industry without it being cyber secure by design, deployed with pro-active and agile vulnerability management and a transparent cyber risk relationship between supplier and end-user.

2.4 Alongside cross-industry action to improve cyber security, efforts must also be made to drive down the costs of cyber security. As an international industry with a broad-spectrum of organizations, everything that can be done to reduce the complexity, cost, or challenge of appropriately managing cyber security risk will ensure that No Country (or company) will be left behind.

2.5 The industry must also do more to pro-actively seek visibility into cyber security risk and vulnerability. This means being open and pro-active to collaboration across stakeholders including peers, nations, multi-national organizations, other sectors and the research community. As an industry, we must be very clear on who our adversaries are and who they are not; those that wish to help us understand our risk are not our adversaries. Cross-sector, legal, private research into hardware and software cyber vulnerabilities has led to a thriving and active research community of those acting in good faith to help multiple industries be more cyber secure.

2.6 The aviation sector is duty bound to listen to, assess and action as appropriate any potential safety issue, howsoever they are notified; we must treat notification of potential cyber security vulnerabilities in same manner. The aviation industry must take steps to build trust and relationships with the research community so that collaborative understanding is built on both sides. IATA additionally supports this effort as well as the generation of measures and legislation that promote and protect the ability of good faith researchers to support the aviation industry.

2.7 During the IATA Aviation Cyber Security Roundtable held in Singapore in April 2019, international attendees from across the sector highlighted both where progress is being made as well as where more effort was required. The salient points are laid out below.

2.7.1 Offered perspectives on the current state of aviation cyber security were;

a) The scale and complexity of aviation cyber security risk is proving challenging for some organizations to understand, prioritize and action.

b) Due to the interdependent and global nature of the aviation sector, it is assessed that cyber security incidents could likely scale rapidly and cause impacts internationally.

c) There remain inconsistencies and insufficiencies across the aviation sector in finding, managing and communicating about cyber security vulnerabilities, leading to poor visibility of actual cyber security risk.

2.7.2 Perspectives on what the attendees saw as the ideal 'Future Vision' for aviation cyber security in 2030 and how to achieve it were proposed as;

a) Cyber Security Culture. Much like a safety culture and a physical security culture, the whole aviation sector needs a cyber security culture.

b) Transparency and Trust. Between all aviation sector stakeholders, there needs to be increased transparency and therefore trust, on cyber security issues ranging from access to cyber security relevant data to secure development practices and vulnerability management. To do this, the aviation sector can apply similar approaches to what it already does across safety and security culture, bringing commonality of approach and ethos in a way that is understood by all.

c) Building consensus and consistency. Across the global aviation sector we need to further build cyber security consistency, standards and governance. This will take organizational and individual leadership as well as a willingness for an open dialogue across all stakeholders.

d) Communications and collaboration. To better manage aviation cyber security risk globally, stronger relationships must be built across the aviation sector as well as with those outside the sector that can assist. This will then foster closer collaboration on everything from developing best practices to managing potential vulnerabilities.

e) Workforce. Through dialogue of the cyber security challenges and opportunities facing the aviation sector, we must inspire a new generation of individuals and organizations that are able to support in answering the aviation cyber security challenge. Additionally, aviation personnel must be taught how to recognize and manage cyber security risks, leading to increased vigilance and resilience.

2.8 Two additional topics were discussed at the IATA Aviation Cyber Security Roundtable.

2.8.1 Investigating the cyber security aspects of accidents or incidents. In the investigation of aviation accidents and incidents there is currently very little visibility of potential cyber security concerns. At a time where many aviation systems are connected and digitized, it was felt that more efforts needed to be made to understand the how to capture, robustly protect and analyze cyber security relevant data. Not to do so means that the industry will have very little ability to assure itself and its customers about its ability to manage cyber security risk.

2.8.2 In summary, there is much to do to increase the cyber safety, security and resiliency of the aviation industry. But alongside this challenge there is much potential for cross-sector collaboration and action, in close partnership between all stakeholders. What we need now is commitment, leadership and action.

— END —