Cyber Security and Resilience Symposium
Summary outcome

(Amman, Jordan, 15-17 October 201)

ICAO MID

CYBER SECURITY AND
RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019

ICAO 2019
75 YEARS OF
CONNECTING
THE WORLD

Symposium Objectives

The main objectives of the Cyber Security and Resilience Symposium were to:

- address cyber security from three different perspectives (AVSEC, ANS and IT);

- raise awareness about cyber threats, risks, challenges and solutions;

- foster a cyber-security culture that promotes a resilient and secure cyberspace; and

- provide a forum for sharing experience and best practices.

Attendance

- 128 Participants

- 23 States

- 6 International Organizations

- 8 Exhibitors/Sponsors

Agenda

Session 1: Setting the scene

Session 2: Cyber Threats and Risks in AVSEC

Session 3: Cyber Threats in Air Navigation Services

Session 4: IT Cyber Threats and Risks

Session 5: Cyber Resilience Pillars

Session 6: Building Resilience: Vendors Perspective

Session 7: Four parts approach to Cyber Resilience

Session 8: Building Cyber Resilience: Regulations Perspective

Session 9: Emerging Cyber Technologies and Solutions

Session 10: Cyber Security Management Framework

Session 11: Outcome

ICAO MID

CYBER SECURITY AND RESILIENCE SYMPOSIUM
TOWARDS A RESILIENT AVIATION CYBERSPACE
AMMAN, JORDAN | 15-17 OCTOBER 2019

ICAO 2019
75 YEARS OF CONNECTING THE WORLD

Challenges

- Tremendous growth in passenger numbers and air traffic
- Rise of cyber attacks including Data breach/malware attack/cloud abuse/hacking/ransomware
- Cyber Terrorism – a new cyber warfare
- Fraud
- Complex infrastructure
- Multiple stakeholders
- Lack of regulatory framework
- Lack of cybersecurity expertise/training
- Lack of ICAO definition for cyber security

ICAO MID

CYBER SECURITY AND
RESILIENCE SYMPOSIUM
TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019

ICAO 2019
75 YEARS OF
CONNECTING
THE WORLD

Challenges cont.

- Lack of budget and resources
- Dynamic, fast moving, evolving nature of cyber attacks makes effective mitigation challenging
- Emerging technologies are more and more interconnected and data-dependent
- ANS Systems' vulnerabilities, systems commonality and emerging technologies and SWIM implementation
- Constantly evolving attacks, quickly evolving threats landscape.
- Obstacles facing Operational Technology (OT)/Internet of Thing (IoT) cyber in airports
- Securing sensitive data

ICAO MID

CYBER SECURITY AND RESILIENCE SYMPOSIUM
TOWARDS A RESILIENT AVIATION CYBERSPACE
AMMAN, JORDAN | 15-17 OCTOBER 2019

ICAO 2019
75 YEARS OF CONNECTING THE WORLD

Recommendations

- States to establish a cyber security culture supported by leadership and guided by example

- States to develop/implement a cyber security strategy

- Global collaboration & strategic alliances to strengthen regional cyber security in addressing cross-border cyber attacks and cyber crimes

- States to adopt more proactive and holistic approaches in order to stay ahead of cyber threats.

- States to ensure that aviation critical systems are secured by design (concept; design; development; delivery; operations; and maintenance)

- States to establish legislative and regulatory framework with enforcement policy

- States to ensure cross-functional coordination by involving relevant domains (AVSEC, ANS, IT, Airports, Airlines, etc);

- States to recruit and retain a talent pool of technical cyber security specialists;

Recommendations cont.

- ICAO to develop additional aviation cyber security guidelines
- States to integrate cyber security architecture and threat intelligence system
- Treat cybersecurity as part of an organizational wide risk management framework, considerate of all applicable domains
- Encourage States to ratify the Beijing Protocol (2010)
- States to avoid prescriptive/descriptive regulations on cyber security
- States to develop contingency/disaster recovery plans as part of the resilient aviation ecosystem
- States to carry out table top exercises on regular basis, with ICAO support, as appropriate
- CAAs are encouraged to collaborate with their National Computer Emergency Response Team (CERT) for cross industry incident management, as appropriate;
- States/Stakeholders are encouraged to use the ATM Data Security Portal (www.adscportal.ae) to share their experience and best practices related to cybersecurity