ICAO UNITING AVIATION

Outcome of the Cyber Resilience Tabletop Exercise

History of the Workshop

- Hosted by Jordan CARC
- Eighty-four (84) participants from seven (7) States (Iraq, Jordan, Qatar, Saudi Arabia, Tunis and United States) and 1 Organization (IATA)

Objective

The objectives of this exercise are to empower participants with measures to mitigate the exploitation of critical Air Navigation Systems, develop awareness on cyber issues affecting aviation, and foster a culture that promotes a secure and resilient use of the cyberspace.

Summary of discussions

1- The Workshop was apprised of the Regional activities on the Cyber Resilience.

2- The Workshop was apprised of the Global challenges for Cybersecurity and what actions ICAO was undertaking to address them.

3- The workshop was presented with three (3) scenarios involving different aspects of Aviation Cyber security and Cyber resilience, which included ATM information sharing disruption, Senior leadership social engineering and Airport notification systems interference

4- The workshop demonstrated global benefits for the aviation ecosystem by being part of IATF by reviewing actual Unmanned Aviation System (UAS) operation use cases related to a broad range of aviation stakeholders.

1st Scenario: An airline is missing flight plan acknowledgements from enroute ANSPs. Airline keeps submitting the flight plans till they get an acknowledgement. Flooding/Duplicated Flight Plans into the FPL processing (FDP) and also surveillance data sharing.

2nd Scenario: The media is aware of the issue going on. ANSP leadership tries to coordinate a common response. The issues within the ATM infrastructure have undermined the capacity of the system by 50%. .

3rd Scenario: Capital City Airport (Flight Information Display Sub-System-FIDS malfunction) (Boarding delays due to no-show passengers at the gate and passenger are being directed to incorrect gates)

5- The Workshop noted that the International Aviation Trust Framework (IATF) aims to enable trusted, secured, and resilient A/G, G/G and A/A data exchange between all stakeholders; furthermore, it was apprised of the core principles and benefits of the IATF;

6- The Workshop was apprised of UAE's activities related to ANS Cyber Resilience including, but not limited to, establishment of Security Operation Center (SOC), continuous enhancement of the ADCS portal and conduct of various training/workshops;

7- The National Cyber security center in Jordan briefed the Workshop on the role of cybersecurity in advancing digital transformation, Cyber dependency and Risk management process.

The Workshop celebrated the international day of ATSEP (12 November 2022)

Recommendations

- States to develop disaster recovery plans as part of the resilient aviation ecosystem; the plan should consider communication, coordination and management oversight to support decision-making.

- States to develop Cyber incidents management plan including defining clear lines of communication and escalation.

- States to promote Cyber awareness training for all staff and in particular senior management recognizing that social engineering and Phishing continue to be a leading vector of attacks, humans are always the weakest link.

- CAAs are encouraged to collaborate with their National Computer Emergency Response Team (CERT) for cross industry incident management, as appropriate;

- Cyber Resilience is an evolving issue and States should include it in ANS contingency plan and to ensure that Contingency plan is known and practiced.

- Cyber Resilience related procedures, risk analysis, exercises and trainings should be established and implemented;

- An agreement on procedure on more timely coordination between FAS (ATSU) and airlines for abnormal flight plan submission is required

- States to perform drills, practice and have lessons learned on a regular basis, with the participation of all internal and external Stakeholders including senior management;

- States to ensure regular coordination between regulators, ANSPs, airport operators and airlines regarding Cyber Resilience;

- Contingency plan should be in place which including back up system and condition for manual procedure

- States to support implementation of Network monitoring, in particular monitoring of:
  - ✓ external links (external to the system)
  - ✓ security incidents specially during cases of cyber attacks; and
  - ✓ fault reporting and advance notification of maintenance activities
- The experts to deal with cyber security/safety issues of ATM systems should be consisted of IT expertise as well as necessary knowledge on ANS and operational process;

ICAO


North American Central American and Caribbean (NACC) Office
Mexico City
South American (SAM) Office
Lima
ICAO Headquarters
Montréal
Western and Central African (WACAF) Office
Dakar
European and North Atlantic (EUR/NAT) Office
Paris
Middle East (MID) Office
Cairo
Eastern and Southern African (ESAF) Office
Nairobi
Asia and Pacific (APAC) Sub-office
Beijing
Asia and Pacific (APAC) Office
Bangkok
THANK YOU