CYBER SECURITY AND RESILIENCE SYMPOSIUM

TOWARDS A RESILIENT AVIATION CYBERSPACE

AMMAN, JORDAN | 15-17 OCTOBER 2019

ICAO MID

Shawn Goudge

Regional Manager Aviation Security, Africa & Middle East

International Air Transport Association (IATA)

Integration of AVSEC and Cyber Security

- Cyber Security and AVSEC
- IATA Initiatives on Cyber Security
  - Working Paper on Cyber Security
  - IATA Cyber Security Position
  - IATA Aviation Cyber Security Roundtable
- Cyber Security – Complexity & Connectivity
- Cyber Security – Integration with AVSEC – A Security Management Systems(SeMS) Approach

Cyber Security and AVSEC

Cyber Security and AVSEC

- Aviation Cyber Security is more than Information Technology Security.
- Aviation Cyber Security (cyber security that pertains to maintaining safe, secure and resilient flight operations), remains a key priority for the sector.
- The interconnectivity between information technology and other processes show that aviation security and cyber security should not be in individual silos and need to be integrated and cyber security vulnerabilities need to be considered in the AVSEC risk assessment process.

Cyber Security and AVSEC

- “Aviation Cyber Security” may be defined as cyber security pertaining to aircraft and airport operations.

- Aviation Cyber Security may be considered as the convergence of people, processes and technology that come together to protect civil aviation organizations, operations and individuals from digital attacks.

- Understanding that not all risks can be known or fully mitigated, adequate resilience to digital attacks and ensuring the continuance of safe aviation operations is a key element of cyber security.

IATA Initiatives On Cyber Security

ICAO Global Aviation Security Plan (GASeP)

- In September 2016, delegates at the 39th Session of the International Civil Aviation Organization (ICAO) Assembly agreed that there was a need for the accelerated development of a Global Aviation Security Plan (GASeP) as a future aviation security policy and programming framework.
- The GASeP, which replaces the ICAO Comprehensive Aviation Security Strategy (ICASS), addresses the needs of States and industry in guiding all aviation security enhancement efforts through a set of internationally agreed priority actions, tasks and targets.
- The GASeP provides the foundation for States, industry, stakeholders and ICAO to work together with the shared and common goal of enhancing aviation security worldwide and achieving five key priority outcomes, namely:

a) enhance risk awareness and response;

b) develop security culture and human capability;

c) improve technological resources and innovation;

d) improve oversight and quality assurance; and

e) increase cooperation and support.

GASeP Specific Measures / Tasks Related to Cyber Security

- Identify and address cybersecurity threats to civil aviation’s critical infrastructure, data and information and communication technology systems through collaboration using horizontal, cross-cutting and functional approaches to achieve an acceptable and commensurate cyber resilience capability on a global level.
- It should involve air navigation, communication, surveillance, aircraft operations and airworthiness and other relevant disciplines to ensure the safety and security of civil aviation operations in full alignment with ICAO’s Global Air Navigation Plan (GANP) and Global Aviation Safety Plan (GASP).
- When considering aviation security risks and measures, ensure appropriate holistic consideration of the aviation sector. Where relevant, early and appropriate coordination with aviation safety, air navigation and facilitation experts to take place at global and national levels.

IATA Aviation Security Strategy and Objectives for Implementation of the GASeP

- IATA has identified 5 Aviation Security Strategy and Objectives for implementation of the GASeP, with the fifth priority related to cyber security:
  - Strategic P5 - Develop an industry-led Cyber/digital security strategy with the core focus on preventing and defending against intentional acts of electronic interference and/or acts of unlawful interference.

IATA Submission to ICAO on Cyber Security

IATA has presented a Cybersecurity working paper to ask that the ICAO 40th Assembly:

- 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 growth and innovation as well as restricting the ability to assess and manage aviation cyber security risk within and across borders.
- This working paper encourages ICAO to, *inter alia*:
  - Recognize the findings from the IATA Aviation Cyber Security Roundtable.
  - Promote the generation of a cyber security culture across the aviation sector following the same model as safety and security culture.
  - Build dialogue, consensus and consistency on both the risks and solutions to aviation cyber security across all international stakeholders, including senior decision makers and risk owners.

IATA Cyber Security Position

IATA Internal Governance and Structures

- As part of the formal IATA governance the newly formed IATA Security Advisory Council (SAC) will advise and guide IATA towards answering the cyber security challenges and opportunities faced by IATA and its airline members.

- The SAC will identify pain points, endorse the development of SARPs as well as speak with one voice to improve cyber security posture and reduce complexity.

IATA Aviation Cyber Security Strategy and Vision

- In consultation with IATA leadership, members and industry partners, an IATA Aviation Cyber Strategy and Vision is to be developed.
-
- Alongside the IATA Aviation Cyber Security Strategy and Vision, a delivery roadmap will lay out how the strategy is delivered.

- https://www.iata.org/policy/Documents/aviation-cyber-security-position.pdf

IATA Cyber Security Position

Stakeholder Engagement

- IATA will engage with its members, industry leaders and stakeholders to develop and subsequently communicate the IATA role and vision in global aviation cyber security.

- IATA will ensure that appropriate partnerships are established that will enable the IATA Aviation Cyber Security Strategy and Vision to be delivered.

Aviation Cyber Security Action

- Taking industry insight, gained during the successful IATA Aviation Cyber Security Roundtable, held in April 2019 in Singapore, some actionable short-term cyber security steps and actions should be identified and conducted by IATA.

- This will not only assist in reducing of cyber security risks but also ensuring that levels of safety and security remain high during the digital transformation of our industry

- https://www.iata.org/policy/Documents/aviation-cyber-security-position.pdf

IATA Aviation Cyber Security Roundtable

- 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.
- 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.

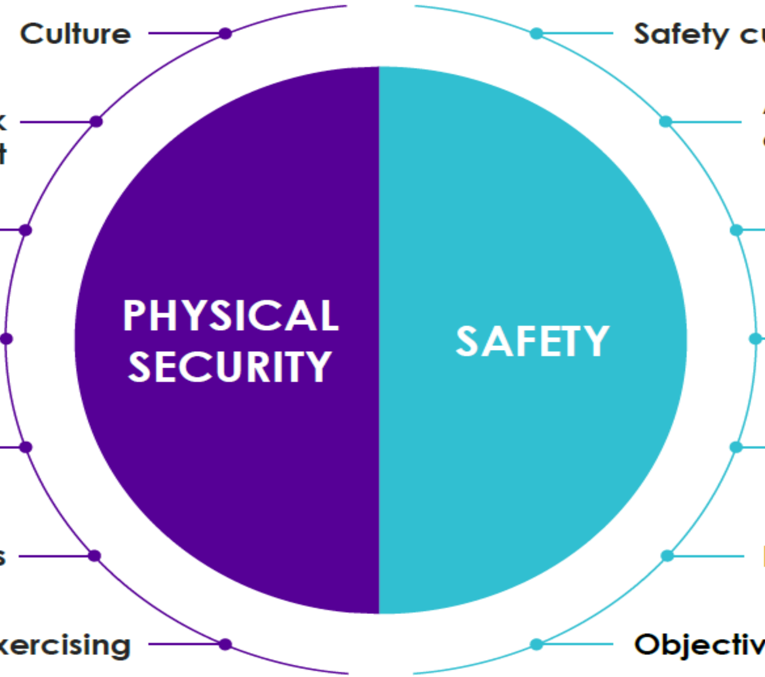
c) There remain inconsistencies and insufficiencies across the aviation sector in finding, managing and communicating about cyber security vulnerabilities, leading to poor visibility of actual cyber security risk.

Future Vision for Aviation Cyber Security in 2030

- 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.
- c) Building consensus and consistency. Across the global aviation sector we need to further build cyber security consistency, standards and governance.
- 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
- e) Workforce. Aviation personnel must be taught how to recognize and manage cyber security risks, leading to increased vigilance and resilience.

Cyber Security – Complexity & Connectivity

Aviation sector benefits from its DNA…

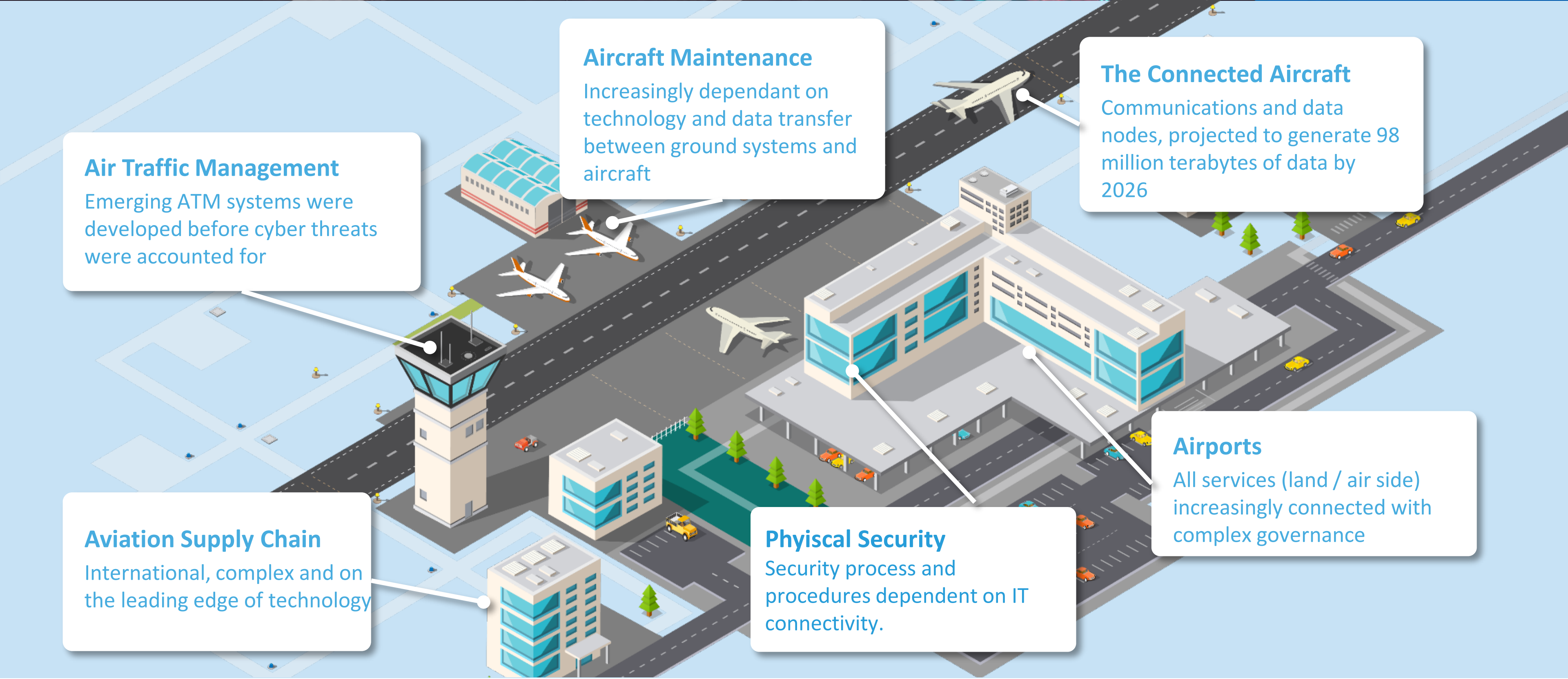


PHYSICAL SECURITY

- Culture
- Mature accountability and risk management
- Robust international standards
- Pro-active to emerging risks
- Timely information sharing
- Dedicated security teams
- Objective testing and exercising

SAFETY

- Safety culture "everyone's responsibility"
- Accountability, governance, objectivity
- 'One in a billion' risk of catastrophic system failure
- Risk – 'ALARP'
- Timely information sharing
- Dedicated safety teams
- Objective root cause analysis of incidents



Aircraft Maintenance

Increasingly dependant on technology and data transfer between ground systems and aircraft

The Connected Aircraft

Communications and data nodes, projected to generate 98 million terabytes of data by 2026

Air Traffic Management

Emerging ATM systems were developed before cyber threats were accounted for

Airports

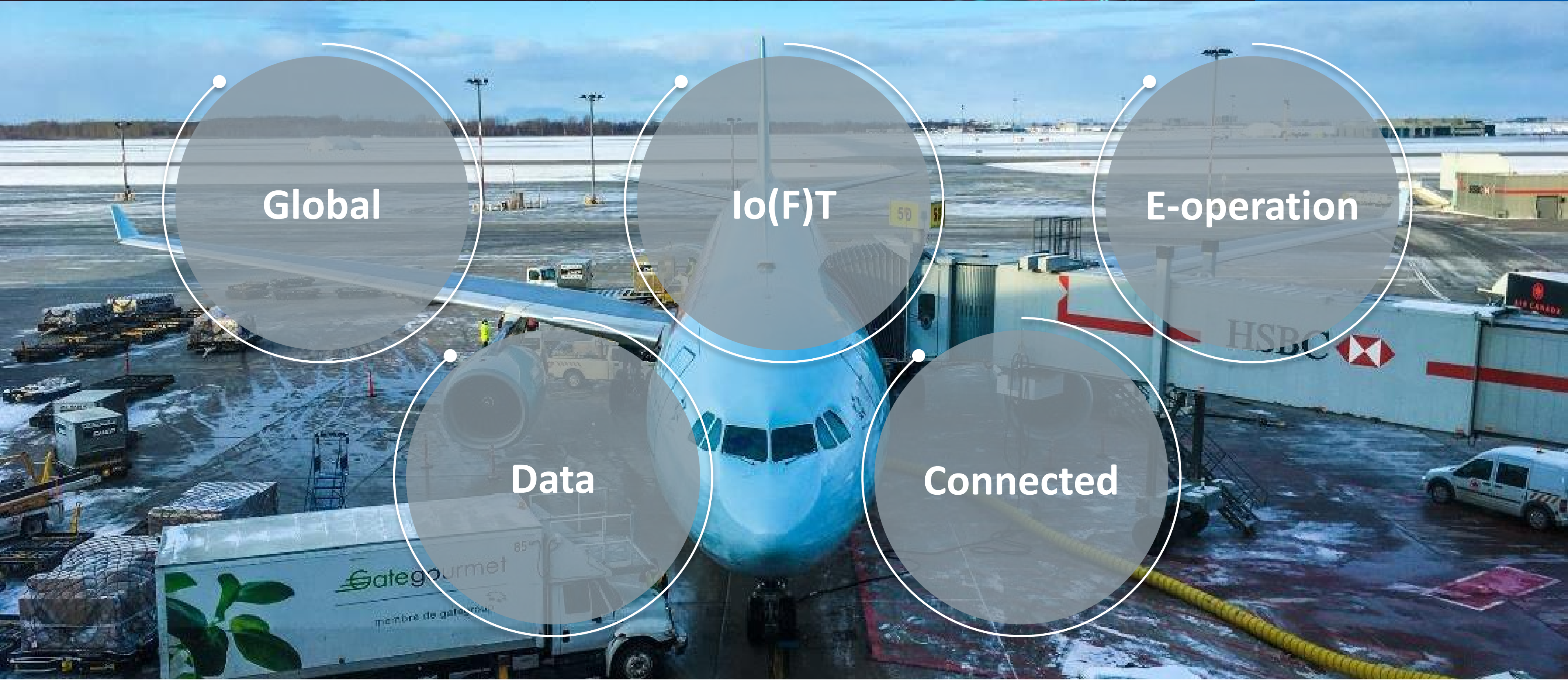
All services (land / air side) increasingly connected with complex governance

Aviation Supply Chain

International, complex and on the leading edge of technology

Phyiscal Security

Security process and procedures dependent on IT connectivity.



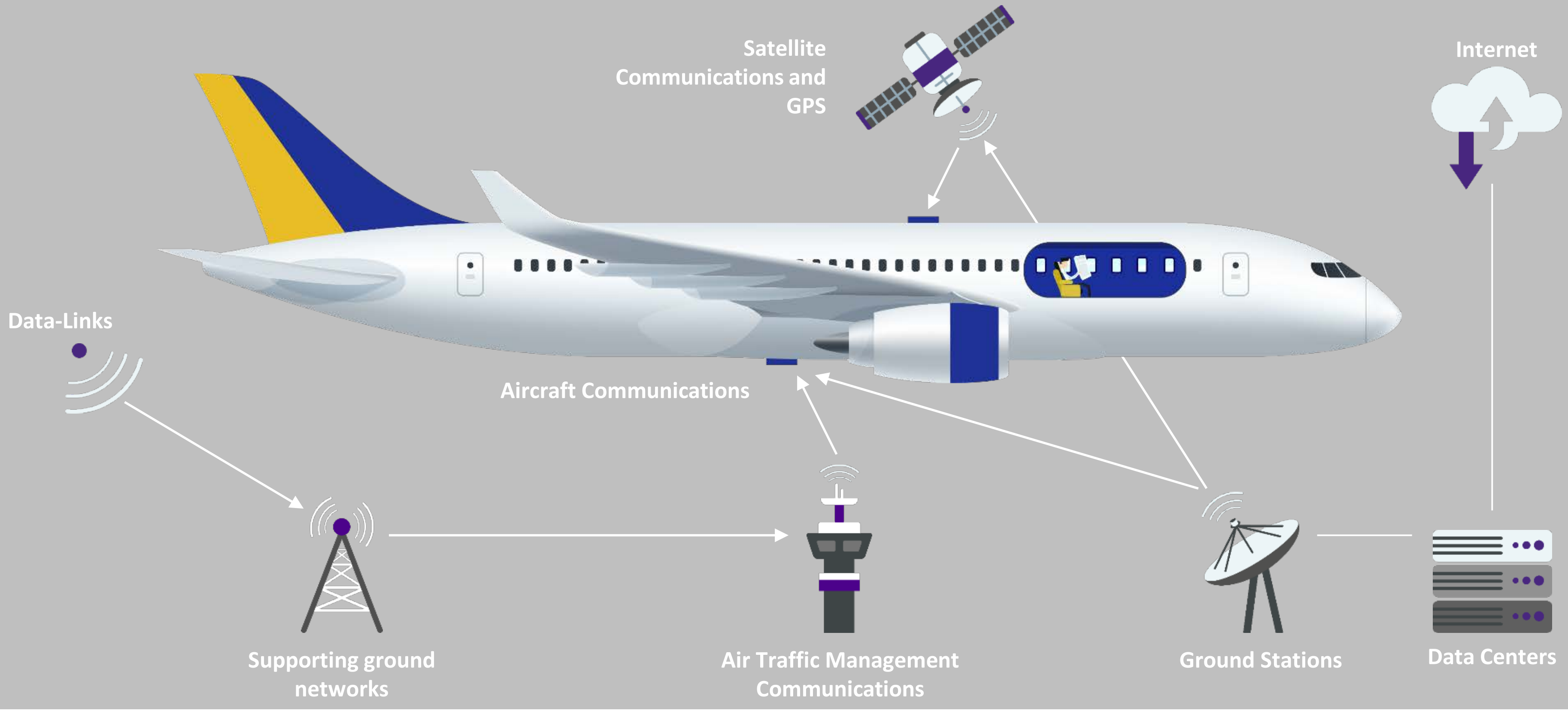
Global

Io(F)T

E-operation

Data

Connected


Satellite Communications and GPS
Internet
Data-Links
Aircraft Communications
Supporting ground networks
Air Traffic Management Communications
Ground Stations
Data Centers

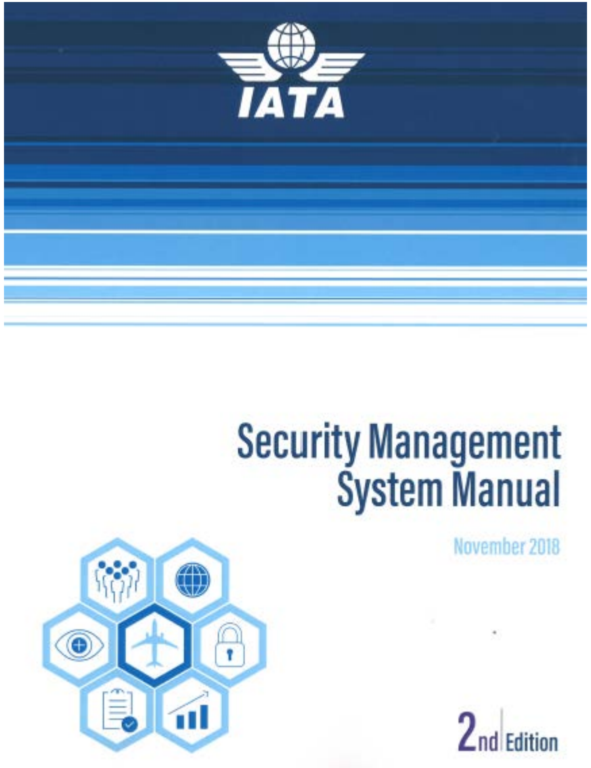
Cyber Security – Integration With AVSEC – A Security Management Systems (SeMS) Approach

Security Management Systems (SeMS) Approach

- A Security Management System (SeMS) is a structured and standardized approach to implementing security processes that provides a uniform level of security throughout the aviation industry. It is performance-based and sets out security results that are measurable and auditable.
- IATA believes the SeMS model can also be applied to the management of cyber threats and risks. The guidance below aims at assisting organizations with the following:
  - Establishing an organizational structure for internal aviation cyber management
  - Identifying areas of importance for implementation of robust cyber policies
  - Providing recommendations about how to address certain aspects of cyber security in the conduct of operations

AVSEC and SeMS

- IATA provides further guidance to its membership in the form of the Security Management System Manual (2nd Edition, November 2018).
- Aviation Security also forms a component of the IATA Operational Safety Audit (IOSA).
- Security Management System (SeMS) is based on the proven principles of Safety Management System (SMS) and enhances airlines security.
- SeMS strengthens corporate commitment and security culture by way of using systematic, data-driven mechanisms of the security reporting and risk assessment which are based on awareness and training and afterwards embedded into the day-to-day business routine.



IATA

Security Management System Manual

November 2018

2nd Edition

Relationship Between AVSEC & Cyber Security

- They key to cyber security from an aviation security (AVSEC) perspective is that cyber and information-technology need to need to be integrated with existing AVSEC processes and procedures.

- This is particularly important where AVSEC functions rely on computers, networks and other information-technology functions.

- All areas outlined in an air operator security program (AOSP) need to be examined from a cyber-security perspective.

- Threat Risk Assessments for aviation security should consider cyber-threats and not just physical threats when being conducted.

- Mitigation strategies should include responses to cyber security risks.

Cyber Security Threats to On-Board Systems

- **Central Maintenance System (CMS)—**The system is connected to the avionics and any data issue will prevent the aircraft from operating.
- **Electronic Flight Bag**—This complicated suite of applications is perhaps the most advanced cyber threat against on-board systems since many airlines are launching programs that utilize tablets or laptops.
- **Flight Management System (FMS)—**An element of the aircraft's “brain”, the FMS is connected to various flight systems as well as avionics and connectivity. There is a potential impact from data corruption or upstream attack on this system.
- **Avionics**—With ongoing connections to aircraft flight controls and integration with connectivity, avionics are associated with the same vulnerabilities as the FMS.
- **Electronic Logbook**—As a maintenance-specific component on the aircraft, there is the potential disruption of operations from a cyber attack.
- On-board Server—The server is a potential vulnerability to many cyber attacks.
- **Navigation Systems**—ADS-B has been identified as being potentially vulnerable to several types of cyber threats as is the NextGen approach in both Europe and the Americas because they rely on an increased use of data communications.
- **Aircraft Management Systems:** Many cabins are now electronically managed, which presents novel opportunities for cyber attack.

Cyber Security Threats to Airline Operations Systems and Processes

- **Reservation System**— Denial-of-Service (DoS) and Identity Spoofing
- **Passenger Name Record (PNR) and Customer Relationship Management (CRM)** — Denial-of-Service or compromise of passenger information.
- **Departure Control System (DCS)**— Denial-of-Service (DoS) and Identity Spoofing; Advanced Passenger Information interference; Watchlist interreference. Unauthorized boarding of passenger.
- **Airline Mobile Applications**— Spoofing attacks and data privacy concerns.
- **Frequent Flyer Systems**—Already viewed as an airline financial liability due to fraud.
- **Flight Planning**—Impact the operation of aircraft across the system.
- **Baggage Reconciliation**—Unauthorized or unscreened baggage could be loaded onto the aircraft.
- **Crew Planning**—Crew logistics is a major effort in most airlines and involves a limited number of reserve staff.
- **Back-office Management**—E-mail and other office-based applications are frequently the source of Trojan horse attacks, identity spoofing and other common cyber-attacks.
- **Cargo**—Airlines that provide cargo, the airline is vulnerable to identity spoofing and upstream attacks. Cargo bookings, E-Airway Bills or E-Consignment Security Declarations can be falsified; Unauthorized or unscreened cargo could be loaded onto the aircraft.
- **Catering / Inflight Stores**—Documentation could be falsified, unauthorized catering or stores not subject to security controls could be loaded onto the aircraft.

Cyber Security Threats to Aviation Security Processes

- **Access Control** – access could be provided to unauthorized persons. Doors left in open position.
- **Pass Control** – airport passes could be provided to unauthorized persons.
- **Background Checks** – information could be falsified.
- **CCTV / Intrusion Detection Systems** – systems can be spoofed, threats and unauthorized access cannot be detected.
- **Supply Chain Interference** – unauthorized goods that are not subject to security controls may enter the restricted area of the airport or be loaded onto an aircraft.
- **Passenger Screening** – algorithms on screening equipment (WTMD, FBS, ETD, X-ray) could be manipulated as not to detect threats.
- **Baggage / Cargo Screening** - algorithms could on screening equipment (ETD, X-ray) be manipulated as not to detect threats; or x-ray systems can be set on automatic clear or transit mode.
- **Communications** – systems can be interfered with or completely stopped. Response to security incidents could be adversely affected.

Conclusion

- Aviation Cyber Security should be integrated into the air carrier’s Security Management System (SeMS).
- Cyber threats to all areas of the air carrier’s aviation security system should be considered (and not only focused on Information Technology).
- Cyber Security and Aviation Security need to be integrated and not be in separate silos.
- On aviation cyber security, IATA, along with the airline industry and all other air transport industry stakeholders, faces a complex, critical challenge that is yet to have a clear answer.
- By taking an active leadership role on this challenge, IATA is in a unique position to systemically reduce aviation cyber security risk for its members across the globe, as well as securing the continued growth of air transport by developing a global cyber security framework as well as standards covering the entire supply chain.
- This will fit into an integrated risk management approach combined with threat intelligence and real time information sharing.

- https://www.iata.org/whatwedo/security/Pages/cyber-security.aspx

Thank You

Shawn Goudge
Regional Manager Aviation Security –
Africa and Middle East (AME) IATA
Office: +962 6 580 4200 ext. 1334
Mobile: +962 (0) 7 97 333 971
Email: goudges@iata.org
www.iata.org