Aviation Security
Cybersecurity

Nick Careen
IATA SVP Airport, Passenger, Cargo, Security

11 - 12 December 2019
Digitization & connectivity have advanced efficiency but also vulnerability.

- Aviation is benefitting from new levels of digitization and connectivity
- These technological advancements are creating tremendous opportunities for flight efficiency, customer service, security, operations and the passenger experience—both in the air and on the ground.
- Yet, with new levels of efficiency gained by increased digitization and connectivity, new levels of vulnerability also arise.
- Today’s airlines face an ever-changing field of cyberattacks from criminals of all kinds – state sponsored attacks, hacktivism, cyber-crime etc
So what’s the risk?

Connectivity of aircraft systems—through traditional information technologies, aviation-specific protocols, and RF communications—has extended the attack surface to the aircraft itself, whether on ground or in flight.

In addition, the digital footprint of aircraft has increased and continues to do so; therefore, the question of digital communication between systems, data validity and information/data security (the protection against intentional interference) has become increasingly relevant.

But there is a difference between perceived threat and the reality.

In 2018, Hong Kong-based Cathay Pacific Airlines noticed suspicious activity on its internal network. Investigators discovered that a hacker obtained access to the personal information of 9.4 million customers. Credit card information, passport information and personal details were all exposed.

BA suffered a data breach in 2018, part of which involved user traffic to the BA website being diverted to a fraudulent site. This resulted in customer details being harvested by the cyber attackers. It is estimated that about 500,000 customers’ personal data were compromised.

There have been claims by hackers that they have the ability to hack the passenger domain communications equipment on commercial aircraft and access critical flight systems. This is not the case. No systems critical to flight safety have ever been put at risk.
That's not to rule out the threat, no threat can ever be ruled out 100% but so far manufacturers have confirmed that no systems critical to flight safety have ever been put at risk.
Cybersecurity is top of mind in aviation

Acknowledging the urgency and importance of protecting civil aviation's critical infrastructure, information and communication technology systems and data against cyber threats, ICAO committed to developing a solid cybersecurity framework.

The 40th Session of the ICAO Assembly adopted Assembly Resolution A40-10 – Addressing Cybersecurity in Civil Aviation. The resolution addresses cybersecurity through a horizontal, cross-cutting and functional approach, reaffirming the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber threats and calls upon States to implement the ICAO Cybersecurity Strategy.

ICAO’s vision for global cybersecurity is that the civil aviation sector is resilient to cyber-attacks and remains safe and trusted globally, whilst continuing to innovate and grow through:

- Member States recognizing their obligations under the Convention on International Civil Aviation (Chicago Convention) to ensure the safety, security and continuity of civil aviation, taking into account cybersecurity;
- coordination of aviation cybersecurity among State authorities to ensure effective and efficient global management of cybersecurity risks, and
- all civil aviation stakeholders committing to further develop cyber resilience, protecting against cyber-attacks that might impact the safety, security and continuity of the air transport system.
- The Strategy aligns with other cyber-related ICAO initiatives, and coordinated with corresponding safety and security management provisions. The Strategy's aims will be achieved through a series of principles, measures and actions contained in a framework built on seven pillars:
  1. International cooperation
  2. Governance
  3. Effective legislation and regulations
  4. Cybersecurity policy
  5. Information sharing
  6. Incident management and emergency planning
  7. Capacity building, training and cybersecurity culture
Industry Focus

First global aviation cyber security resolution – step in right direction

Provides global framework for aviation cyber security

Airlines and governments need to continue to work together to understand threats and vulnerabilities

Capacity building is key

- We welcome the establishment of the first Global Aviation Cyber Security Resolution by the Council of the International Civil Aviation Organization (ICAO)
- IATA aims at building capacity, improving efficiency and driving optimization in security systems through;
  - Developing Standards
  - Developing Sensible Regulations
  - Reducing technology gaps
Thank you