Cyber Threat, a Real Challenge for Civil Aviation Industry

Brahim Lakhlfifi
Aviation Consultant
blakhlfifi@gmail.com
Our context today

- Twenty-four hours a day, 365 days of the year, an aircraft takes off or lands every few seconds somewhere in the world.
- Every one of these flights is handled in the same, uniform manner, whether by air traffic control, airport authorities or pilots.
- Behind the scenes are millions of employees involved in manufacturing, maintenance and monitoring of the products and services required in the never-ending cycle of flights.
Our context today

- In fact, modern aviation is one of the most complex systems of interaction between human beings and machines ever created.
- This clock-work precision in procedures and systems is made possible by the existence of universally accepted SARPs.
- SARPs cover all technical and operational aspects of international civil aviation, such as safety, security, personnel licensing, operation of aircraft, aerodromes, air traffic services, accident investigation and environment.
Our context today

Without SARPs, our aviation system would be at best chaotic and at worst unsafe.
Our context today

- The aviation industry is expanding, changing, and becoming increasingly connected;
- The increased connectivity or links between ground systems and some of these ground systems and aircrafts constitute a potential vulnerability if not well designed and protected;
- In our “Multi-stakeholders industry, do we have a common vision, or common strategy, goals, standards, implementation models, or international policies defining cyber security?
Our context today

- **Safety vs security** – There is a widespread opinion that safety management deals with all security issues, but since safety management discounts malicious activity then this is not the case;

- **New technology and lack of experience** – Much of the new IT technology being introduced raises potential security issues which are unfamiliar in the civil aviation industry;

- **Consolidation** – IT systems are becoming increasingly interconnected and interdependent, so organisations are exposed to risks caused by security weaknesses in other people’s systems.
The problem today

- The increased connectivity or links between ground systems and aircraft, as well as the use of commercial off-the-shelf software and hardware, constitute a potential vulnerability;

- Aviation ICT systems need to be upgraded periodically due to changes in operating requirements or software upgrades, and often require modifications in software and/or hardware;

- While the resilience of safety operations is based on redundancy, security equipment is designed on a single point of failure (X-Ray machine or WTMD, for example).
How do we protect?

- Do we have clear provisions (NCASP, ASP, Etc.)?
- Do we know all our critical systems?
- Do we protect the critical systems against unauthorized access and use?
- Do we prevent tampering with the systems?
- Do we have tools to detect attacks on the systems?
- Do we have a reporting system for cyber attack which would facilitate the collection and analysis of information, and the implementation of appropriate countermeasures
ICAO recommends that the physical protection of such systems should begin at the design stage or as early as practicable to ensure that they are as robust as possible against cyber attacks.

ICAO recommends the use of a multilayered approach:

1. administrative controls
2. virtual or logical controls
3. physical controls
How to protect

- Security standards, policy and procedures;
- Threat and risk assessment to identify the vulnerabilities;
- Background checks for maintenance staff, including outsourced maintenance;
- Inclusion of a security provision in the specifications for and procurement of ICT systems;
- Virtual or logical controls.
How to protect

- System hardware, particularly servers, is appropriately secured and located in areas to which access is controlled;
- Only those authorized to have access are accessing the system;
- Limiting the number of persons with authorized access;
- Requiring more than one person for approvals within systems;
- Maintaining activity logs, which can be useful in auditing and evaluating.
How to protect

- Networks used for critical aviation information and communication technology systems are separated from networks to which the public has access;
- Routes for cables should be designed so that critical aviation information systems cannot be easily infiltrated;
- Remote access to critical aviation information and communication technology systems is only permitted under prearranged and secure conditions.
The challenge today

- In the past we were focussed on perimeter intrusion detection system (PIDS), lighting or a closed-circuit television (CCTV) system to protect our industry.

- Do we have such intrusion detection system for all of our ICT or security equipment?

- We have SOPs to respond in case of perimeter intrusion, do we have the same for ICT systems intrusion?
The challenge today

- Should we create a new generation of AVSEC officer (2.0) to deal with such threat?

- Should we promote aviation security as an Airport Collaborative Decision Making (A-CDM) process, enabling organised sharing of information between relevant stakeholders in the airport environment, including ANSP?

- Should we promote and establish an alert system to facilitate communication with operators and other stakeholders?
Questions