Cybersecurity from an aviation security perspective

Matthieu Gualino
PhD in political science
Deputy Director - ICAO Aviation Security Training Center
ENAC – French civil aviation university
Plan

1/ Definitions and concepts
2/ Civil aviation and cybersecurity
3/ Cybersecurity governance: aviation security perspective
1/ Definitions and concepts
Aviation security

Safeguarding civil aviation against acts of unlawful interference. This objective is achieved by a combination of measures and human and material resources.
Aviation security

- From an historical point of view, aviation security refers to unlawful acts like:
  - unlawful seizure of aircraft,
  - destruction of an aircraft in service,
  - hostage-taking on board aircraft or on aerodromes,
  - forcible intrusion on board an aircraft, at an airport or on the premises of an aeronautical facility,
  - introduction on board an aircraft or at an airport of a weapon or hazardous device or material intended for criminal purposes,
  - use of an aircraft in service for the purpose of causing death, serious bodily injury, or serious damage to property or the environment
Aviation security

• Some examples
A risk based approach governance

• In order to ensure the identification of appropriate preventive security measures, the level of threat should be continually reviewed and risk assessments carried out, taking into account international, national and regional situations and environments.

• Whenever a specific threat exists, selected and predetermined preventive security measures should be applied, commensurate with the associated risk assessment, and the nature and severity of the threat.

“Cyber” issue is identified as a new risk for aviation security
2/ Civil aviation and cybersecurity
Why Cyber-risks are important in the field of aviation security?

3 Identified vulnerabilities

- ATM
- AIRCRAFT
- AIRPORT
It would be highly offensive and inappropriate to explain you why it’s important
Aircraft cyber security can be defined as the prevention of and/or reaction to deliberate malicious acts undertaken via cyber means to either compromise an aircraft’s systems directly or indirectly where those systems play a key role in the wider aviation system.
Aircraft

- If we consider that an aircraft communicates:

- If we consider that: for example there are 1000 apps which are running when an airbus A380 is in the air
Aircraft

• If we consider that some persons are interested in hacking airplanes vulnerabilities

This issue must be taken into account
What kind of events are considered?

- **Flight Control** – the safety critical systems required to fly the aircraft.
  - Disruption or denial can directly impact safety.
  - **High Impact / Low likelihood**

- **Cabin (Operational)** – the systems used to operate and maintain the aircraft.
  - Disruption or denial mostly impacts business critical operations and possibly maintenance.
  - **Medium Impact / Medium likelihood**

- **Cabin (Passengers)** – those systems / interfaces which the passengers have direct interaction with.
  - Disruption or denial has minimal impact and is considered to be a public area with untrusted devices.
  - **Low impact / High likelihood**
Airport cyber security can be defined as the prevention of and/or reaction to deliberate malicious acts undertaken via cyber means to either compromise an airport’s systems directly or indirectly where those systems play a key role in the wider aviation system.
Airport
Airport

• If we consider that airports are at a crossroad between ATM and aircraft
• If we consider that most of the airport equipment are connected

This issue must be taken into account
What kind of events are considered?

- The scenarios identified fall into two broad categories:
  - attacks that could **facilitate** a conventional attack by degrading aviation security measures (screening, access control etc.) and
  - attacks intended to **disrupt** airport or airline operations, principally around passenger facilitation (such as departure control, baggage handling, etc.).
Aviation Security philosophy toward cybersecurity

- Cybersecurity applied to civil aviation is not new

- There are debates to define if there’s a specific issue to cybersecurity applied to civil aviation

- So... the objectives are:
  - not to “reinvent the wheel” but to adapt existing rules to aviation security regulation
  - Work hand in hand with safety stakeholders
3/ cybersecurity governance: aviation security perspective
What are the groups involved in the governance?

- ICAO Working Group on Threat and Risk
- ICAO Working Group on Training
- ECAC studygroup on cyberthreats to civil aviation
- National CAA groups
- National initiatives
What are the adopted decisions

• Each Contracting State should, in accordance with the risk assessment carried out by its relevant national authorities, ensure that measures are developed in order to protect critical information and communications technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation

• Each Contracting State should encourage entities involved with or responsible for the implementation of various aspects of the national civil aviation security programme to identify their critical information and communications technology systems, including threats and vulnerabilities, and develop protective measures to include, security by design, supply chain security, network separation, and remote access control, as appropriate
What are the adopted decisions?

- The appropriate authority should ensure there are procedures in place to identify and assess cyber risks to civil aviation. This should include all relevant stakeholders for example in the intelligence agencies, control authorities and industry in that country. On the basis of that analysis they should ensure that appropriate measures are in place to:
  
  a) mitigate the likelihood of those threats occurring;
  b) recognise them when they do occur; and
  c) respond to and therefore limit the consequences of such attack.

ECAC DOC30
THANK YOU!
MERCI!

Matthieu Gualino
matthieu.gualino@enac.fr