INFORMATION SECURITY
VS. CYBERSECURITY
THE CANSO VISION FOR A SUSTAINABLE AND EFFECTIVE INTEGRATED LAYER TO THE DIGITAL ERA BRIDGING SAFETY AND SECURITY
Francesco Di Maio
**CANSO Vision 2020 security strategy:**

“The introduction of increased automation and reliance on system-wide exchange of data means that the associated cyber-security issues are now a key area that requires joint industry solutions. ICAO has initiated activities in this area and CANSO will develop a work programme to identify common ANSP policies in the security area”.

“Security refers to the protection against threats that stem from intentional acts (e.g. terrorism) or unintentional acts (e.g. human error, natural disaster) affecting aircraft, people or installations on the ground. Adequate security is a major expectation of the ATM community and of citizens. The ATM system should therefore contribute to security, and the ATM system, as well as ATM-related information, should be protected against security threats. Security risk management should balance the needs of the members of the ATM community that require access to the system, with the need to protect the ATM system.”
Being realistic...

From this...  To this... and much more
What’s new?

The digital (r)evolution: we are now living in a fully interconnected, digitalized, interoperable environment.

Threat scenario changes:
- sophisticated enemies + state sponsored attacks;
- evolving terrorists;
- high tech availability and low prices;
- new vulnerabilities affecting Hardware and Software;
- interdependencies and domino effects;
- reconsider some weaknesses: internal threats and contractors/subcontractors/consultants...
Operational Concept

While traditional enterprise approach tends to protect business continuity, ANSPs’ call of duty is to play a role in protecting human life, service continuity and fundamental rights connected to flying.

The provision of air traffic services, as envisaged by this Regulation, is connected with the exercise of the powers of a public authority, which are not of an economic nature justifying the application of the Treaty rules of competition. Actually, that activity constitutes a service in the public interest which is intended to protect both the users of air transport and the populations affected by aircraft flying over them (Reg. EC 550/2004; EC Commission in the case C 364/92 SAT Fluggesellschaft mbH v Eurocontrol)

Information Security is one of the major drivers to ensure the safety and regularity of air traffic services provision.
Which means:...

Information Security is not (only) matter of IT but involves:

• Organization (commitment+roles+responsibilities)
• People → culture
• technology

Holistic approach required;

Stop talking only about threat, let’s work on VULNERABILITIES (think to Secure software);

Bear in mind the evolution (e.g.: SWIM)
Some hints: at EU level

4. SECURITY

Air navigation service providers shall establish a security management system to ensure:

(a) the security of their facilities and personnel so as to prevent unlawful interference with the provision of air navigation services;

(b) the security of operational data they receive or produce or otherwise employ, so that access to it is restricted only to those authorised.

The security management system shall define:

(a) the procedures relating to security risk assessment and mitigation, security monitoring and improvement, security reviews and lesson dissemination;

(b) the means designed to detect security breaches and to alert personnel with appropriate security warnings;

(c) the means of containing the effects of security breaches and to identify recovery action and mitigation procedures to prevent reoccurrence.

Air navigation service providers shall ensure the security clearance of their personnel, if appropriate, and coordinate with the relevant civil and military authorities to ensure the security of their facilities, personnel and data.

EC REGULATION 1035/2011 Ann.I Para 4
amended and repealed by EC Reg 373/2017

(d) Air navigation services and air traffic flow management providers and the Network Manager shall take the necessary measures to protect their systems, constituents in use and data and prevent compromising the network against information and cyber security threats which may have an unlawful interference with the provision of their service.

Including specific needs for:
- Considering security by design and through lifecycle
- Identify potential impacts of security breaches toward Safety
- Training on information security aspects for «ATSEP» (Air Traffic Safety Electronics Personnel);
- Definition of liability and accountability for post-holders and accountable manager

RISK BASED APPROACH
NIS Directive (Transport Sector)

Article 5

Identification of operators of essential services

1. By 9 November 2018, for each sector and subsector referred to in Annex II, Member States shall identify the operators of essential services with an establishment on their territory.

2. The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows:

(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;

(b) the provision of that service depends on network and information systems; and

(c) an incident would have significant disruptive effects on the provision of that service.

3. For the purposes of paragraph 1, each Member State shall establish a list of the services referred to in point (a) of paragraph 2.
Article 14

Security requirements and incident notification

1. Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

3. Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

RISK BASED APPROACH
To ensure prevention, detection, reaction and recovery referred to any event that could jeopardize the safe and secure provision of air traffic services and to preserve the human life on board and on the ground, the efficiency, regularity and the confidence on transportation by air.
COMPLIANCE + DUE DILIGENCE

- Being merely compliant with the regulatory requirements doesn’t mean to be diligent
- Having a security management system means to be aware of risks and vulnerabilities and act to fix
- Governance is critical for Security Management System’s effectiveness
- *Not prevent an event, when exists a legal duty to prevent it, is equivalent to causing it (e.g.: art. 40 Italian Criminal Code)*
- Liability is based on what organizations do before – not after – a security breach;
- Compliance and diligence cannot be delegated
- Due diligence must be always proved with evidences.
Conclusions

- CANSO believes that Information Security in civil aviation should be demystified and reverted to a consistent operational concept in which:
  - Sinergy should be a primary value → public/private partnership;
  - Rules are clearly defined;
  - Strategies are defined, made sustainable and cost-effective → risk based approach;
  - Funding issues are honestly discussed and fixed;
  - Critical factors are identified and involved (e.g. non-aeronautical entities, such as telco and energy)
  - Human factor is definitely understood and addressed
In this corner, we have firewalls, encryption, antivirus software, etc. And in this corner, we have Dave!!
Thank you!

CANSO Headquarters
Transpolis Schiphol Airport
Polaris Avenue 85e
2132 JH Hoofddorp
the Netherlands

tel: +31 (0)23 568 5380
fax: +31 (0)23 568 5389
email: info@canso.org