canso POLICY

CANSO Position Paper on Cyber Security

CANSO Europe Region Office 24.09.2014

canso
civil air navigation services organisation

CANSO Europe Region Office
Wetstraat 82 Rue de la Loi, 1040 Brussels, Belgium.
Tel: +32 (0)2 201 0911 Fax: +32 (0)2 203 8916 email: Europe@CANSO.org

CANSO Position Paper on Cyber Security

1. Introduction

As defined by the International Telecommunications Union (ITU-T X.1205) "Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment."

Cyber security strives to ensure the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the cyber environment. Generically the following should be considered:

- Availability
- Integrity, which may include authenticity and non-repudiation (ensures that a message has been sent and received so a sender/receiver cannot later deny having sent/received the message)
- Confidentiality

2. Background and Context

Historically the bulk of communication between ANSPs has been using point to point links to exchange information between bespoke systems hosted within each ANSP. These solutions have worked, but are expensive with long development times and an inflexible solution. This is changing with the adoption of international (IT) networking and architectural standards as well as the use of Commercial Off The Shelf (COTS) based open systems mirroring commercial IT practice.

Programmes such as SESAR, NextGen and the Japanese Collaborative Action for Renovation of Air Transport Systems (CARATS) have all been designed to take account of these weaknesses.

The intention of this position paper (CANSO Europe Interoperability Task Force) is to assist the CANSO Policy Steering Group and CANSO Aviation Security Workgroup to form a CANSO global position.

3. Cyber Threat facing ATM

The cyber security threat facing ATM has many facets:

- As ATM moves towards open standards and systems ANSPs will become increasingly vulnerable to cyber attack. To counter this, ANSPs need to become more knowledgeable about the threats they face and more flexible and responsive in their actions to counter them.

- The dissemination of expertise from the expert virus writers into toolkits that can be used by anyone is accelerating. For example once Stuxnet (Worm used to attack Iran's nuclear program) was identified, it was rapidly grabbed and altered at code level and redistributed by top level virus writers. It was then incorporated into cybercriminal tool kits and sold over the "Darknet".

- The cyber world is of increasing interest to criminals and like the drugs cartel they are creating a professional standard, geographically distributed supply chain to conduct cyber warfare.

4. The way forward for ATM Cyber Security

Any ATM-specific cyber security strategy should include the following key points:

1. Any strategy should define the requirement, not a "one-size fits all" solution. It should be straightforward; not add an unnecessary burden of complex documentation or be expensive to maintain and audit.

2. ATM organisations use existing International standards such as ISO27001:2013 that can be independently audited against (Europe has EN16495 which references ISO/IEC27001 and ISO/IEC27002). They can tailor this standard, if necessary, thereby removing the need to develop a specific ATM one.

3. The guidance produced by groups such as the National Institute of Standards and Technology (NIST), or ISO28000 which has been used by some European organisations. This includes a maturity level assessment that can be used to define an ATM-specific information security management system (ISMS).

4. Using an International standard and guidance, a generic ATM profile identifying how ATM organisations such as ANSPs should interpret the standard can be developed and agreed by the relevant organisations such as CANSO and ICAO.

5. A risk-based approach based on ISO 27001:2013 or the NIST Cyber Security Framework (http://www.nist.gov/cyberframework/index.cfm), along with external audits, will allow ANSPs to measure progress, assess gaps and demonstrate compliance, without changing the way they do business and reuse processes supporting other functions e.g. change management.

6. All groups within ATM should share information, intelligence and research where applicable (to include State and possibly open source) so that effort isn't duplicated, recognising that this requires a protected forum.

7. Security should be considered at the highest level of each organisation and not just at an individual system level due to the discrete approach that the latter approach provides. For SESAR this means at the EATMA level (European ATM Architecture).

8. There should be coordination across all groups within ATM e.g. ANSPs, the military, the State, CANSO Global, ECAC, standardisation bodies, SESAR, NextGen, CARATS, airlines, airports, airframe manufacturers, national and international security operations centres (e.g. in Europe, EUROCONTROL's Security Assessment Team proposal for Centralised Services) and system providers. This will enable the roles and responsibilities of the various stakeholder groups to be defined in a common way along with suitable, globally defined, guidance material to protect the whole ATM industry from attack.

9. ATM can learn from other industries that also have a safety culture such as process control, energy, and other major infrastructure providers, where security has relied on obscurity and legacy, and which are moving to open standards and systems.

10. ATM needs to develop and maintain a level of cyber security expertise within the industry and each organisation.

5. Recommendations and Conclusion

CANSO recommends that:

- ATM organisations implement security in accordance with ISO 27001:2013, and ensure alignment with it
- Use an information security framework (for example NIST) and a generic ANSP profile to measure maturity and demonstrate compliance
- Develop trust mechanisms to enable the exchange of cyber threat and attack information so that the industry can protect itself
- Organise an integrated cyber exercise, utilising experience from the military exercises already undertaken, to test our preparedness
- Work across industry and internationally to implement a common cyber security vision, strategy, goals and frameworks

CANSO – the Civil Air Navigation Services Organisation – is the global voice of air traffic management (ATM) worldwide. CANSO Members support over 85% of world air traffic. Members share information and develop new policies, with the ultimate aim of improving air navigation services (ANS) on the ground and in the air. CANSO represents its Members' views to a wide range of aviation stakeholders, including the International Civil Aviation Organization, where it has official Observer status. CANSO has an extensive network of Associate Members drawn from across the aviation industry.

For further information, please contact:

Guenter Martis - Director European Affairs
CANSO Europe Region Office
Wetstraat 82 Rue de la Loi, 1040 Brussels, Belgium
Tel: + 32 (0) 2 201 0911 - Fax: + 32 (0) 2 203 8916 - Europe@CANSO.org