In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

CYBERSECURITY CONSIDERATIONS FOR AVIATION

Mayda Ávila S.

Regional Officer, Communications, Navigation and Surveillance International Civil Aviation Organization North American, Central American and Caribbean Regional Office-ICAO

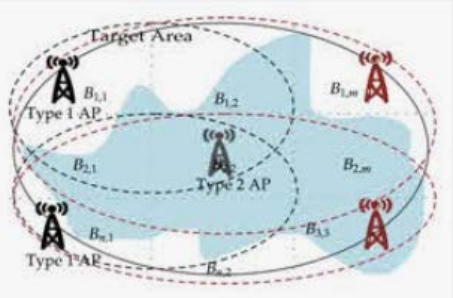
In cooperation with

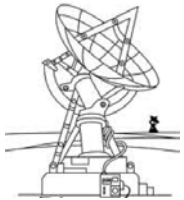
ICAO

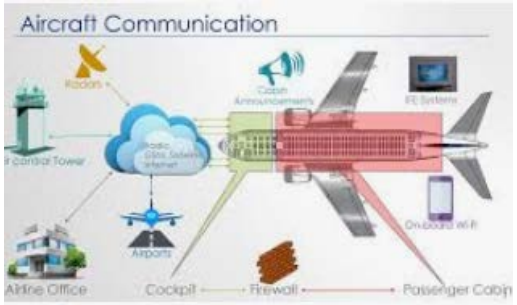
canso
civil air navigation services organisation

AIRBUS

Our sector which includes airspace users, air navigation service providers, airport operators, civil aviation authorities and original equipment manufacturers, was targeted by attackers for several reasons, but especially for financial gain and intellectual property theft, also to decrease safety in the aeronautical operations.







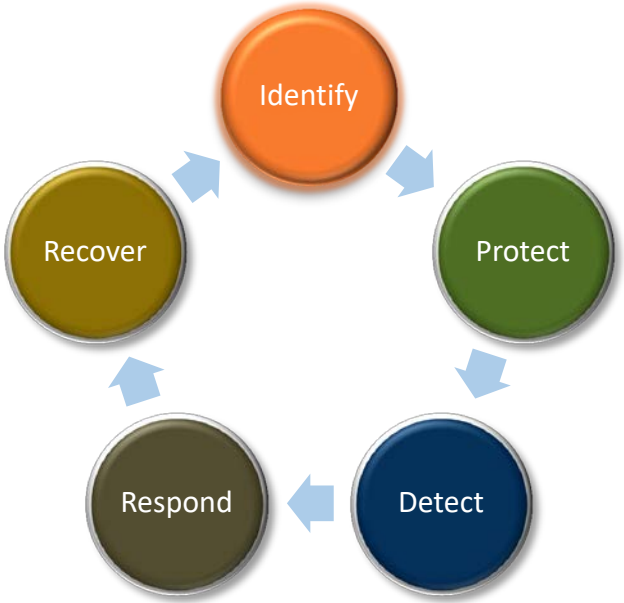
In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Best Practices about Cybersecurity



- CANSO Standard of Excellence in Cybersecurity.
- International Telecommunication Union (ITU)National Cybersecurity Strategy Guide.
- National Institute of Standards and Technology framework (NIST) of United States.

In cooperation with

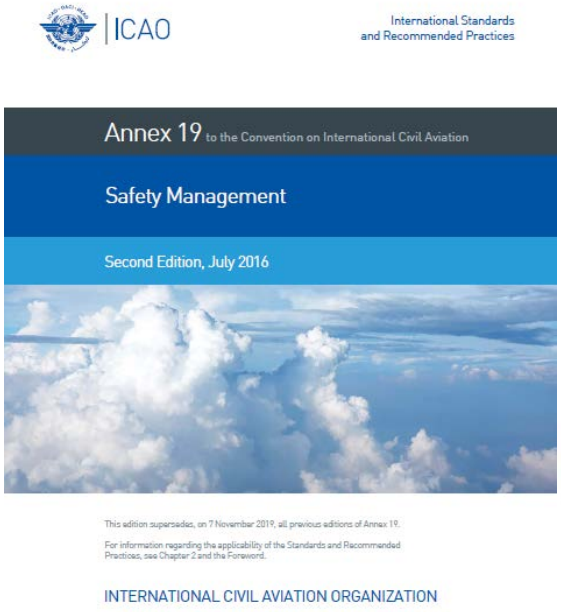
ICAO

canso
civil air navigation services organisation

AIRBUS

Identify

- Identify vulnerabilities and risk about your organization.
- The organization understands the cybersecurity risk to organizational operations.
- ANSPs should conduct a risk assessment to determine the greatest risks to the organization and business.
- Safety data and safety information collection, analysis protection, sharing and exchange information.
- Risk management must have to be an important process inside of any organization.



Risk Management

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Protect

- Protect the critical elements of your organization.
- Identify what elements need protection from others than cannot be protected.
- Protect include many kinds of barriers, hardware, software also people.

Protect in depth is a simple principle for defining the architecture for your cybersecurity strategy. While no one technology or security activity is perfect, the presence of many independent layers of defenses will increase the difficulty for attackers and decrease the chances of a successful attack.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

The process of identifying assets, classifying, and implementing protection measures is therefore an essential component of a cybersecurity Programme.

An effective asset management Programme will help to enhance cybersecurity via the appropriate discovery and analysis of assets. Assets include data, devices/systems, facilities and people.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Detect

- Be sure that you have or are undergoing a cybersecurity event.
- Detected in a timely manner and the potential impact of events is understood.
- Detecting and identifying anomalous activity.
- Development procedure and actions to detect.
- Be proactive.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Respond

- You detect a cyber-attack; What are you going to do?
- Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
- Respond include respond planning and mitigation.

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

Recover

- Recovery plan in place.
- Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
- A recovery can be as small as from a single malware incident through to a complete disaster recovery scenario.
- Planning all procedures, mitigations and resources required are key to building a sound recovery solution regardless of the scale of the incident.

Effective measures to evaluate the different processes must be put into operation.

"Remember that what is not measured cannot be improved"

In cooperation with

ICAO | canso civil air navigation services organisation | AIRBUS

The Human Element of Cybersecurity

- *The Internet of Things.*
- *Making your people an essential part of cyber security strategy of any organization.*
- *Create a cybersecurity culture.*
- *Talk the same language about cybersecurity.*

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

The Human Element of Cybersecurity

- *An incident can be due to both an external entity and an internal entity.*
- *Internally events can be intentional or due to human error.*
- Elements such as adequate training should be part of the cybersecurity strategy.
- Information security is not only a matter of technology.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Activities under ICAO Regional Offices

- Training with the support of Eurocontrol in the management of AMHS databases and addressing.
- Training by the industry in the management and configuration of the ATC system databases.
- Management of aeronautical frequencies at a regional level to ensure that they are protected for current and future services.
- Strengthening of regional communication networks through new projects that increase safety.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Conclusion

- Cybersecurity Strategy include identification of all stakeholders, understand and manage all aviation operations, implement effectives procedures in all cybersecurity approach process and provide adequate resources to support the process.
- Cybersecurity approach must have to be guidance by policies and directives, governance that comes from high level of the organization.
- Responsibilities have to be stablish in all cybersecurity process.
- Adequate training and knowledge of the personal have to be stablish.
- Risk management and measure/improve process to ensure security controls as a way to better measure and manage our risk.
- Common language in which you can talk about cyber risk a way to measure it.

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

Documents

- ICAO Annexes
- ICAO Document 8973 - Aviation Security Manual
- ICAO Document 9985 – ATM Security Manual
- ICAO Aviation Cyber Security Strategy
- ICAO Document 9849- GNSS Manual
- ITU National Cybersecurity Strategy Guide
- CANSO Standard of Excellence in Cybersecurity
- ISO 27000 Series of Standards
  - ISO/IEC 27001 Information Security Management
  - ISO/IEC 27002:2013- Information technology — Security techniques — Code of practice for information security controls.
- ICAO website: https://www.icao.int/cybersecurity/Pages/default.aspx
- FAA website: https://www.faa.gov/air_traffic/technology/cas/
- EUROCONTROL website: https://www.eurocontrol.int/cybersecurity
- NIST website: https://www.nist.gov/cyberframework/framework

“Coming together is a beginning, keeping together is progress, working together is success.”

Henry Ford

Next events

- Webinar about ICAO NACC Cybersecurity Manual
  February 2021
- Cybersecurity Workshop
  Second semester of 2021, La Havana, Cuba

In cooperation with

ICAO

canso
civil air navigation services organisation

AIRBUS

MONTRÉAL
(HEADQUARTERS)

PARIS
(EUROPEAN AND
NORTH ATLANTIC)

BEIJING
(ASIA-PACIFIC
SUB-OFFICE)

CAIRO
(MIDDLE EAST)

MEXICO CITY
(NORTH AMERICA AND CARIBBEAN)

DAKAR
(WESTERN AFRICA)

BANGKOK
(ASIA-PACIFIC)

NAIROBI
(EASTERN AFRICA)

LIMA
(SOUTH AMERICA)

THANK YOU!