AVIATION CYBERSECURITY STRATEGY

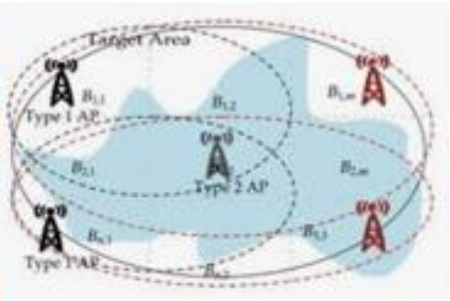
THE VISION OF A GLOBAL AVIATION CYBERSECURITY STRATEGY

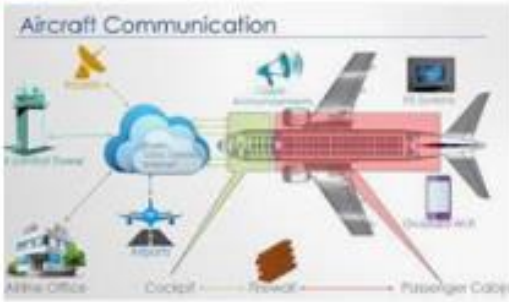
Mayda Alicia Ávila

Communication, Navigation and Surveillance

ICAO NACC Regional Officer

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.





Aviation is a “system of systems”

Intentionality!

Cybersecurity requires close coordination between aviation safety and aviation security

Background

- Assembly Resolution A39-19 instructed ICAO to develop a comprehensive cybersecurity work plan and governance structure;
- Secretariat Study Group on Cybersecurity (SSGC) developed the Cybersecurity Strategy endorsed by the ICAO 40th Assembly (Resolution A40-10 – Addressing Cybersecurity in Civil Aviation, superseding Resolution A39-19).

A40-10: Addressing Cybersecurity in Civil Aviation

- Calls upon States and industry stakeholders to take the following actions to counter cyber threats to civil aviation:
  - Implement the Cybersecurity Strategy
  - Identify the threats and risks from possible cyber incidents on civil aviation operations and critical systems.
  - Define the responsibilities of national agencies and industry stakeholders.
  - common understanding among Member States of cyber threats and risks.
  - government/industry coordination with regard to aviation cybersecurity strategies.
  - robust all-round cybersecurity culture.
  - development and implementation of international standards, strategies and best practices on the protection of critical information

ICAO Cybersecurity-Working Groups

https://www.icao.int/cybersecurity/Pages/Working-Groups.aspx

Working Group on Cybersecurity for Flight Safety: to address cyber safety, security, and cyber resilience aspects of airworthiness.

Research Sub-Group on Legal Aspects: Ensure adequacy of the existing international legal framework to address cyber threats against civil aviation and to review the draft Cybersecurity Strategy.

Working Group on Air Navigation Systems: To address cyber safety, security, and cyber resilience aspects of current and existing airport, air navigation and information management systems

Working Group on Airlines and Aerodromes: addresses cybersecurity matters related to airport and airline operations.

ICAO Cybersecurity Strategy

- INTERNATIONAL COOPERATION
- GOVERNANCE
- EFFECTIVE LEGISLATION AND REGULATION
- CYBERSECURITY POLICY
- INFORMATION SHARING
- INCIDENT MANAGEMENT AND EMERGENCY PLANNING
- CAPACITY BUILDING, TRAINING AND CYBERSECURITY CULTURE

Aviation cybersecurity needs to be harmonized at the global, regional and national levels in order to promote global coherence and to ensure full interoperability of protection measures and risk management systems.

https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx

ICAO NACC Cybersecurity Approach

- *Create a team; Integrate a Security (AVSEC) and Air Navigation Activities.*
- *Evaluation about new Technologies and interconnections between CAR States.*
- *Integration of different Stakeholders such as States with more experiences, Organizations and Industry to have a regional approach.*
- *Create a ICAO/NACC-CANSO-AIRBUS cybsercurity approach for CAR States.*
- *More than one year of work starting on March 2020 with three different phases:*
  1. *Development of a common languages.*
  2. *Presentation of the cybersecurity Policy Manual*
  3. *Direct support to CAR States*

In cooperation with ICAO canso AIRBUS

WHY USE "POLICY" AS A SECURITY CONTROL?

These technical protections need to build on a solid foundation:

Risk Management

Business is about **managing risk**, so this is about managing security in a way that is familiar and well understood.

Regulation

Aka **Governance** – independent oversight to help keep the right behaviours happening.

Maintenance

Protecting against **supply chain** attacks via maintenance partners

Comms Security

Protecting against **impersonation** and **being influenced** by anonymous attackers

Access Control

Both **physical** and **logical**, use of least privilege, etc.

Handling Incidents

Consider an incident might be an **intelligent attacker** rather than a statistical event.

Think about **Business Continuity**, maybe graceful degradation of service.

Also consider **Disaster Recovery** – how to rebuild from nothing.

Share knowledge and **work together** - even commercial competitors are on the same side against attackers.

New Systems

Design in **foundational security**, and make sure **procurement chains** are trustworthy and not compromised

Ops Security

Building good cyber into operational processes

Compliance

Maintaining **evidence packs** – a key part of Audit

Asset Management

Knowing what you have, and what vulnerabilities you might be exposed to

Is There any Example For "Good" Policy

Of course! The "Air Traffic Management Cybersecurity Policy Template"

Developed in partnership by ICAO, CANSO and Airbus:

CONTEXT

Risk Management:

- Consider security throughout all risk management
- Have a methodical process to give justifiable decisions
- Integrate security across the entire lifecycle

Asset Management:

- Know what you have
- Control access and be proportionate to IT/OT/IACS/Comms
- Recognise the value of data as well as physical assets

Supply Chain:

- Map the entire end-to-end chain
- Start at adjacent links and work out
- Mitigate using Risk Management

Incident Response:

- Prepare and consider Informed Attackers
- Define priorities based on scenarios
- Share information with partners

OBJECTIVES

Risk Management & Governance

- Management SECTION 7
- Regulation SECTION 8
- Compliance SECTION 20

Protecting Assets

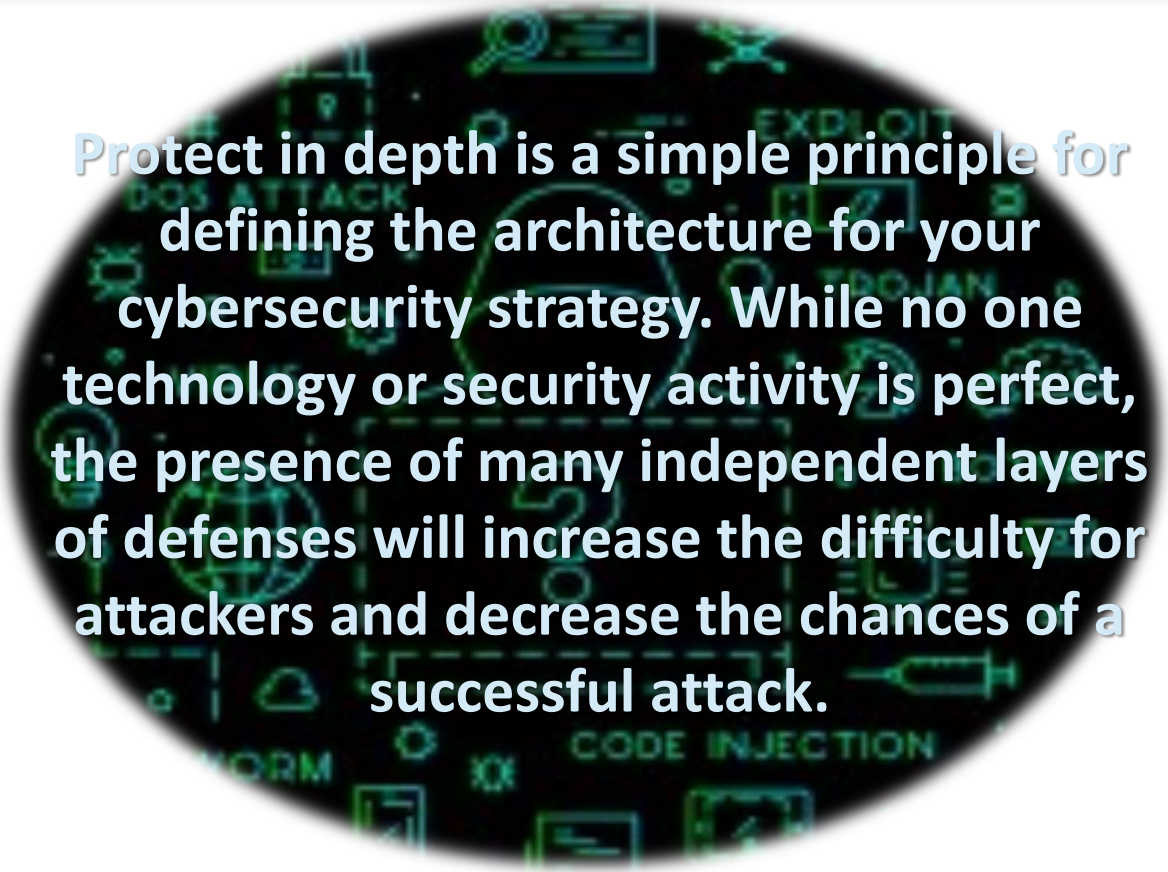
- Asset Management SECTION 10
- Operational Security SECTION 13
- Access Control SECTION 11
- Communication Security SECTION 14

Supply Chain

- Maintenance SECTION 15
- Acquisition SECTION 15
- Relationships SECTION 16

When things go wrong...

- Incident Management SECTION 17
- BC / DR SECTION 18
- Speaking out SECTION 18



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.

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.

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

“Remember that what is not measured cannot be improved”

Conclusions

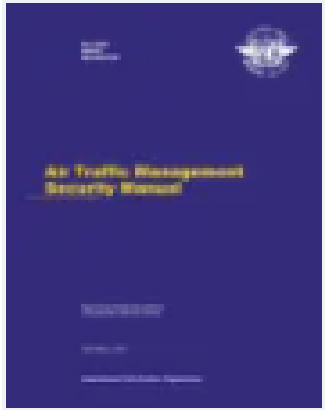
- Cybersecurity Strategy include identification of all stakeholders, understand and manage all aviation operations, implement effectives procedures in all cybersecurity approach process and provide adequate resources to support the process.
- Cybersecurity approach must have to be guidance by policies 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.

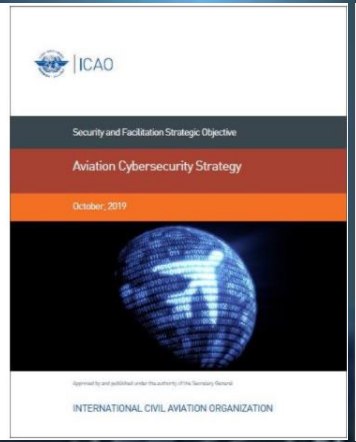
"Coming together is a beginning, keeping together is progress, working together is success."

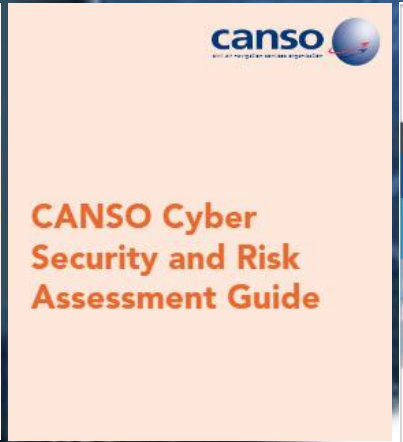
Henry Ford

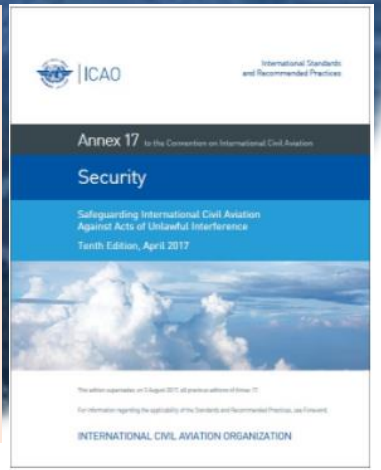
Documents


ICAO
Doc 8973 — Restricted
Aviation Security Manual
INTERNATIONAL CIVIL AVIATION ORGANIZATION



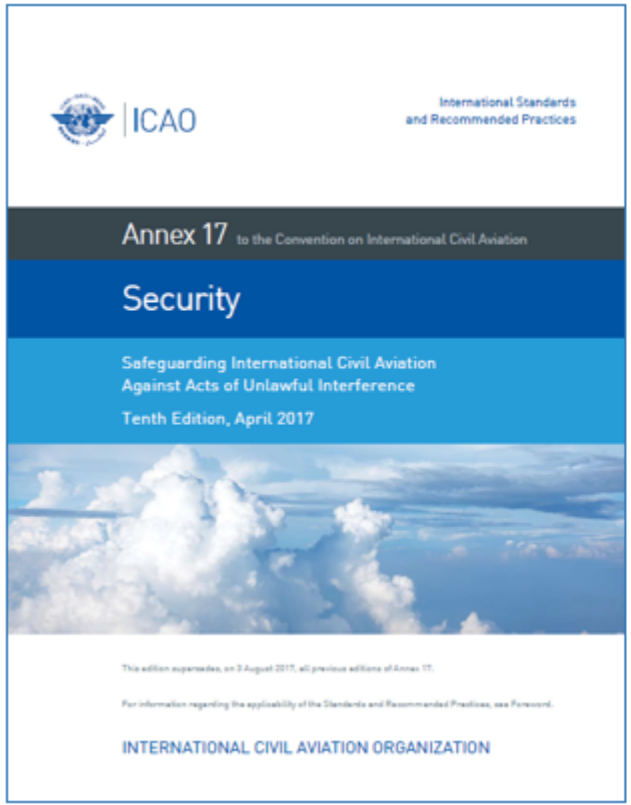

ICAO
Security and Facilitation Strategic Objective
Aviation Cybersecurity Strategy
October, 2019
INTERNATIONAL CIVIL AVIATION ORGANIZATION


canso
CANSO Cyber Security and Risk Assessment Guide


ICAO
International Standards and Recommended Practices
Annex 17
Security
Safeguarding International Civil Aviation Against Acts of Unlawful Interference
Tenth Edition, April 2017
INTERNATIONAL CIVIL AVIATION ORGANIZATION

Documentation

- *Resolution A40-10: Addressing Cybersecurity in Civil Aviation*
- *Air Traffic Management Cybersecurity Policy Template.*
- *Safety Management Manual (SMM) (Doc 9859).*
- *ICAO Aviation Security Global Risk Context Statement (Doc 10108)*
- *Aviation Security Manual (Doc 8973)*
- *Annex 17: Security Provisions*



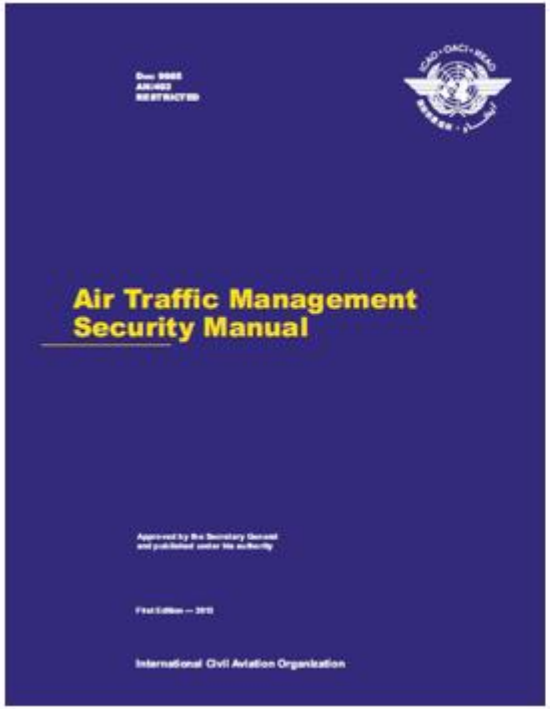
Acts of unlawful interference

Communication of false information such as to jeopardize the safety of an aircraft in flight or on the ground, of passengers, crew, ground personnel on the general public, at an airport or on the premises of a civil aviation facility.

Measures relating to cyber threats

4.9.1 Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference.

4.9.2 Recommendation – *Each Contracting State should ensure that measures implemented protect, as appropriate, the confidentiality, integrity and availability of the identified critical systems and/or data. The measures should include, inter alia, security by design, supply chain security, network separation, and the protection and/or limitation of any remote access capabilities, as appropriate and in accordance with the risk assessment carried out by its relevant national authorities.*



ATM security definition

(ICAO Circular 330, Civil/Military Cooperation in Air Traffic Management)

The contribution of the ATM system to civil aviation security, national security and defense, and law enforcement; and the safeguarding of the ATM system from security threats and vulnerabilities.

ATM security has dual requirements of protection of the ATM system against threats and vulnerabilities and the provision of ATM security services in support of organizations and authorities engaged in aviation security, national security, defense, and law enforcement.

Documentation

- *Air Traffic Management Security Manual (Doc 9985)*
- *Annex 19; Safety Management.*
- *ICAO Aviation Cybersecurity Strategy*
- *CANSO Standard of Excellence in Cybersecurity*
- *ISO/IEC 27000-series comprises information security standards*
- *ICAO Cybersecurity Action Plan*

ISO/IEC 27000-series comprises information security standards

- **Information about best practices to improve information security**

- ISO/IEC 27000 Information security management systems Overview and vocabulary
- ISO/IEC 27001 Information security management systems Requirements
- ISO/IEC 27002 Code of practice for information security management
- ISO/IEC 27003 Information security management system implementation guidance
- ISO/IEC 27004 Information security management Measurement
- ISO/IEC 27005 Information security risk management
- ISO/IEC 27006 Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27010 Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications.

ISO/IEC 27000-series comprises information security standards

- **Information about best practices to improve information security**

- ISO/IEC 27011 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27031 Guidelines for information and communications technology readiness for business continuity
- ISO/IEC 27033-1 Network security overview and concepts
- ISO/IEC 27033-3:2010 Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
- ISO/IEC 27035 Security incident management
- ISO 27799 Information security management in health using ISO/IEC 27002


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)
ICAO

THANK YOU!