How a global industry player addresses the Cybersecurity challenges of Air Transport

ICAO Cyber Summit and Exhibition
Making Sense of Cyber
Dubai, United Arab Emirates
4 – 6 April 2017

thomas.hutin@thalesgroup.com
www.thalesgroup.com
Air Transport Cyber-attack surface is growing

More interconnected systems means more reachable targets

Increasing Connectivity and use of non-protected by design A/G Data Link Communication

More access points with networking and System Wide Information Management (SWIM) for CDM

Migration for interoperability to standard IP-based network with publicly available vulnerabilities

Less isolated architectures with e-enabled aircrafts, clouded services, virtual center and remote processing, Total Airport Management...
Cyber-attacks are multiplying in many sectors

- **Destructive attacks**
  - TV5 Monde, Ukraine power grid attack...

- **Denial of service attacks**
  - Boryspil Airport (Kiev Ukraine), Indonesian targets including airlines and airports (to protest against Air pollution), Hanoi Ho Chi Minh airports...

- **Information theft**
  - Operation Cleaver (Pakistan, Qatar, Korean airlines, etc.), US Office of Personnel Management...

- **Ransomware**
  - Hospitals, Civil Aviation Authority...
Potential Aviation Threats Actors

- **Nation States**
  - Persons of Interest
  - Offensive operations

- **Criminals**
  - Financial Gain
  - Fraud
  - Ransomware

- **Terrorism**
  - > Destruction
  - < Disruption

- **Hacktivists**
  - Activism
  - Kudos
  - Geopolitics
Lessons learned from other domains

- All victims of cyber attacks had “some cybersecurity counter-measures in place”
- Cyber-attacks are detected today through side effects
- Rebuilding a system is no easy task and back-up systems won’t probably help
- Cyber-analysis including testing, attack simulation & exercise are best practices
- Full protection is not achievable, anticipation, detection & resilience are recommended

A successful Cyber-attack can cost up to tens of M$

> Immediate direct cost due to service interruption for hours or days
> Indirect cost for investigation and “clean” rebuilding
Cyber threats in air transports?

Surveillance & Navigation infrastructure

Operational Control Center (OCC)

Maintenance Control Center (MCC)

Airport

ANSP

Aircraft data & parts supplier & third Party
How to integrate new e-enabled aircrafts in my IT system without impairing safety or operations?

Did I take into account the cyber risks in my Safety Management System?

How do I operate the security functions of my connected aircrafts? (Operational Manual)

Do I have cybersecurity in my ERP (Emergency Response Plan)?

Am I ready to detect cyber attacks during flight?

How to integrate IATA recommended practices on cybersecurity?

How to protect passengers data?

Impacts of connectivity and e-enabled aircrafts for the airlines?
Growing cyber-risks are rising questions to many ANSP

- As critical operator, how to cope with strengthening regulation in particular for legacy systems?
- Is my surveillance network a major weakness? Or elsewhere?
- What is the safety and operational impacts of cyber-attacks?
- Does contingency planning enough to be resilient against serious attacks?
- What is my policy about cyber-incident and more generally about Cybersecurity?
- Does cyber-protection enough? What is the minimum level?
- What kind of training for my staff? Should I organize exercises?
A wide range of cybersecurity challenge for airports operators

- What would be the impacts of modification and unavailability of AODB?
- How to manage cybersecurity of critical SCADA systems?
- What are the impacts of cyber attacks on Security (baggage reconciliation, access control...)?
- How to protect from hybrid attacks?
- How to ensure cybersecurity of IT networks: vital communication services to airport & public access for passengers?
- How to ensure cybersecurity of IT infrastructure to airlines (DCS, PC for load sheet preparation...)?
- How to protect passenger personal data?
The need for coordinated approach

Need to ADAPT and IMPROVE cybersecurity posture

- Cyber-Threats increase
- ATM Cyber-attacks surface increases
- New regulation on cybersecurity

Connected to:
- Civil Aviation Authorities
- Airlines
- ANSP
- Airports
- Manufacturing Industry
Working with you in Air Transport Cybersecurity initiatives

Through International Coordinating Council of Aerospace Industries Associations
- ICAO IHLG with ICAO, IATA, CANSO & ACI (A39-19)
- WP236/Coordinating Cybersecurity work

Civil Aviation Cybersecurity Task Force of
- Discussion with EASA (roadmap and ECCSA)
- Established relationship with ECAC

Member of ARAC ASISP WG
Member of CANSO WG
Member of EU-ISAC
Standardization : WG72, A871, A771…
Our harmonisation expectations for Air Transport

- Cybersecurity evolution for communication standards
  - Asterix, CPDLC, ADS-B, ACARS...

- Framework and guide for assessment, labeling and certification of cybersecurity
  - System
  - Product
  - Component
  - Services

- Policy for vulnerability management
  - Disclosure
  - Awareness
Our internal initiative

Thales combines expertise: domain and cybersecurity

- **Investment** for providing state-of-the-art solutions & services for global Aviation Cybersecurity
- **New solutions & services** dedicated to Air Transport systems
- Integration of Cybersecurity in our engineering process & tool
- Awareness and **Training** of our staff

Our cybersecurity transformation plan to help our customers make cybersecurity an enabler for new usages and services development
What can we do as Thales?

- Leverage experiences from other domains: Defense, Banks, Satellite...
- Provide in-depth cybersecurity (from boundary protection to core components)
- Develops specific solutions through deep domain knowledge
- Propose preventive cybersecurity maintenance
- Feed cybersecurity monitoring with domain Threat Intelligence (*A-ISAC, ECCSA...)
- Support customers with dual expertise team in case of intrusion (Rapid Reaction Team)
Thales experience in Cybersecurity

- 130 customers
- Protection of the world’s banking transactions: 80%
- Cybersecurity specialists: 2,000
- High-grade security products and solutions (confidential or top secret) for 50 countries
- Cybersecurity for 9 of the top 10 internet giants
- Cybersecurity for 19 of the 20 largest banks
- 5 cybersecurity centres
- 5 data centres

Incl. NATO countries