Cybersecurity, safety and resilience - Airline perspective

Rabat, November, 2017

Presented by
Adlen LOUKIL, Ph.D
CEO, Resys-consultants

Outline

1. Vulnerabilities, Cybersecurity recent incidents
2. Aviation Cybersecurity: A New Security Landscape
3. Cybersecurity best practices: ISO and NIST approaches
4. ICAO/ACAC Recommendations
Main sources of GNSS Vulnerabilities

- Ionospheric delay
- Tropospheric delay
- Satellite clock error
- Ephemeris error
- Signal error
- LOS Blockage
- Receiver noise
- Dilution of precision
- Jamming
- Spoofing
Cybersecurity has become an elevated risk that is among the most pressing issues affecting businesses. Today’s cyber adversaries are more persistent, skilled, and technologically savvy than just a year ago, and leaders across all industries are taking notice.

According to PwC’s 2015 Global Airline CEO Survey, 85 percent of airline CEOs view cybersecurity as a significant risk, likely reflecting the highly sensitive nature of flight systems and passenger data.

→ Online attacks are on the rise,
→ For the airline industry, cybersecurity risk is top of mind.
Cybersecurity & Airplane recent incidents
Hackers bombard aviation sector with over 1,000 attacks per month

By Jorge Valero | EURACTIV.com

11 July 2016
Exploiting the problem, researcher Ruben Santamarta said hackers could "hijack" in-flight displays to change information such as altitude and location, control the cabin lighting and hack into the announcements system.
Malaysia suffered cyber-attack after MH370 disappeared

FMT Reporters | April 21, 2015

Cyber security expert claims phishing e-mails were used to infiltrate navy, police and civil aviation departments
On June 21, 2015

LOT Polish Airlines had its flight operations system hacked, resulting in disruption or cancellation of 22 flights. While there is little public information, and indeed there are some conflicting reports as to whether this was an actual cyber security attack, it is reported to have been a Distributed Denial of Service (DDoS) attack on a private network responsible for issuing flight plans, showing the scope for penetration into the inner workings of an airline’s IT estate;
Aviation Cyber Security:  
A New Security Landscape
What’s Cybersecurity?

- **Cybersecurity is**:  
  
  - The collection of technologies, policies, security concepts, processes and best practices designed to protect networks, computers, cyber environment, programs, data and organization from attack, damage or unauthorized,

  - Preservation of Confidentiality, Integrity and Availability of information in the Cyberspace. (ISO 27032, Clause 4.20)
Can cause business high level costs. Despite the financial cost, there can also be reputational damage, causing decrease in level of business or sometimes segment specific or total disruption.
Cybercrime

- Cyber crime encompasses: any criminal act dealing with computers and networks (called hacking). Additionally, cyber crime also includes traditional crimes conducted through the Internet.

- Cybercrime includes:
  - Illegal Access, illegal interception,
  - System and data interference,
  - Misuse of devices
  - Fraud
Infiltration attack vulnerabilities

Categorised according to the ISO27005:2011 Annex D

<table>
<thead>
<tr>
<th>Types</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Lack of periodic replacement schemes</td>
</tr>
<tr>
<td>Software</td>
<td>Well-known flaws in the software</td>
</tr>
<tr>
<td>Software</td>
<td>Poor password management</td>
</tr>
<tr>
<td>Network</td>
<td>Unprotected communication lines</td>
</tr>
<tr>
<td>Personnel</td>
<td>Insufficient security training</td>
</tr>
<tr>
<td>Personnel</td>
<td>Lack of security awareness</td>
</tr>
<tr>
<td>Organization</td>
<td>Lack of formal process for access right review (supervision)</td>
</tr>
<tr>
<td>Organization</td>
<td>Lack of fault reports recorded in administrator and operator logs</td>
</tr>
<tr>
<td>Organization</td>
<td>Lack of records in administrator and operator logs</td>
</tr>
</tbody>
</table>
Cybersecurity best practices: ISO Standards and NIST approach
Alignment with Best Practices

- ISO/IEC 27001 — Information security management systems — Requirements.
- ISO/IEC ISO 22301 — Guidelines for information and communication technology readiness for business continuity
- SO/IEC 27032 — Guideline for Cybersecurity
- NIST: National Institute of Standards and Technology
ISO 27001:2013
Information Security Management System
SITA completes ISO certification for information security at Changi Airport

Location: Singapore

Steve Lee, Chief Information Officer/Senior Vice President, Technology, Changi Airport Group, said: “We congratulate SITA on achieving the ISO 27001 certification. CAG values our partner’s commitment to
GHIAL obtains ISO 27001 2005 certification
Hyderabad | 12 March, 2009

One of the first airports in South and South East Asia

Hyderabad, 12th March, 2009: The auditors of BSI (British Standards Institute) have awarded GMR Hyderabad International Airport Limited (GHIAL) and the Rajiv Gandhi International Airport an ISO 27001:2005 (Information Security Management System) certification. This is the highest certification from BSI for Information Security, which not only consists of IT but also Information Technology and Communications, Human Resource, Facilities and Administration.
ISO 27001:2013 ISMS

Plan
- Traffic Threat Assessment
- Preparation for Incident Response

Protect
- Defensible Network Architecture
- Pervasive Network Awareness
- Network Security Monitoring

Respond
- Network Incident Response
- Network Forensics

Detect
- Network-Centric Security Processes
Security awareness, training and education programs provide many benefits to organizations: (1) Improving employee behavior, (2) increasing employee accountability, (3) mitigating liability for employee behavior, (4) complying with regulations and contractual obligations.
ISO 22301:2011
Business Continuity Management System

ISO 22301 Business continuity management systems. Requirements
UAE's Abu Dhabi International Airport has received the ISO 22301 Management System Certificate for Business Continuity Management.

It becomes the first airport in the Middle East to be ISO 22301 certified, and among the few cities in the world to have achieved this.
Delhi airport acquires ISO-22301:2012

The operator of India's busiest airport, Delhi International Airport (P) Ltd (DIAL) announced that it has become the first airport in the world to achieve ISO 22301:2012 certification.
Benefits to an Organization for Implementing a Business Continuity Management System

- Identify and manage current and future threats to your business
- Take a proactive approach to minimizing the impact of incidents
- Keep critical functions up and running during times of crises
- Minimize downtime during incidents and improve recovery time
- Demonstrate resilience to customers, suppliers and for tender requests
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>Protect</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td>Information Protection Processes &amp; Procedures</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td>Protective Technology</td>
</tr>
<tr>
<td>Detect</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td>Detection Processes</td>
</tr>
<tr>
<td>Respond</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
</tr>
<tr>
<td>Recover</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td>Communications</td>
</tr>
</tbody>
</table>
Risk Management Process
9 Basic steps of Cybersecurity

These are the guidelines to follow while drawing up a comprehensive Cybersecurity program in an Organisation:

• #1: Explore the Legislation and other requirements
• #2: Define the Business benefits and get top Management support (Very Important)
• #3: Setting the Cybersecurity requirements
• #4: Choosing the framework for Cybersecurity Implementation
• #5: Organizing the Implementation (Setting up Teams, PM Resources, Project Charter, Budget etc)
• #6: Risk Assessment & Mitigation (Applying Controls)
• #7: Implementation of Controls
• #8: Training & Awareness
• #9: Continuous Monitoring and Checks and Reporting to Senior Management (C Level Executives)
Airline perspective & Recommendations
International Civil Aviation Organization
WORKING PAPER
AIRCRAFT CERTIFICATION
CYBERSECURITY
REGULATORY EFFORTS
ASSEMBLY — 39TH SESSION
EXECUTIVE COMMITTEE AND TECHNICAL COMMISSION
2/19/2-16

Novembre 2016
Guidelines & best Practices (1/2)
Guidelines & best Practices (2/2)

Cyber Threat Management
Threat intelligence research and data management, SIEM, BigData Analytics, Behavior and Malware Analysis, HoneyPots, Situational Awareness

Security Ops, Asset Mgmt
Policy, Compliance, Manage Security Controls, Vendor Management, Security Standards, Security Architecture, Encryption, Access Control, Assurance

Identify threats, Threat modeling
Incident Response
Risk Assessment, Vuln Management

Organization wide risk strategy, Report Risk
Risk Management

Information Security
1) Aviation sector is increasingly reliant on the:
   - Availability of information and communications technology systems,
   - Integrity and Confidentiality of data,
   - Resilience of the global aviation system to cyber threats;

2) Threat posed by cyber incidents on civil aviation is rapidly and continuously evolving;

3) Cybersecurity issues should be addressed through the application of safety management systems;

4) The importance and urgency of protecting civil aviation’s critical infrastructure systems and data against cyber threats;
5) Define a shared vision, strategy and roadmap to strengthen the global aviation system’s protection from and resilience to cyber threats; and

6) Recognizing the multi-faceted and multi-disciplinary nature of cybersecurity challenges and solutions;

Counter cyber threats to civil aviation:

a) Identify the threats and risks from possible cyber incidents on civil aviation operations and critical systems, and the serious consequences that can arise from such incidents;

b) Define the Responsibilities of national agencies and industry stakeholders with regard to cybersecurity in civil aviation;
c) Encourage the development of a common understanding among Member States of cyber threats and risks, and of common criteria to determine the criticality of the assets and systems that need to be protected;

d) Encourage government/industry coordination with regard to aviation cybersecurity strategies, policies, and plans, as well as sharing of information to help identify critical vulnerabilities that need to be addressed;

e) Systematic sharing of information on cyber threats, incidents, trends and mitigation efforts;
f) Adopt a risk-based approach to protecting critical aviation systems through the implementation of cybersecurity management systems;

g) Encourage a robust cybersecurity culture within national agencies and across the aviation sector;

h) Determine legal consequences for activities that compromise aviation safety by exploiting cyber vulnerabilities;

i) Promote the development and implementation of international standards, strategies and best practices on the protection of critical information and communications technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation;

Establish policies and allocate resources when needed to ensure that, for critical aviation systems: system architectures are secure by design; systems are resilient; methods for data transfer are secured, ensuring integrity and confidentiality of data; system monitoring, and incident detection and reporting, methods are implemented; and forensic analysis of cyber incidents is carried out;
<table>
<thead>
<tr>
<th>PREVENTION</th>
<th>DETECTION</th>
<th>REACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>The first line of defense is to prevent attacks that can corrupt or destroy data and interrupt operations. We presented key elements of attack prevention that include:</td>
<td>Even with the best prevention systems, determined hackers will get through. It’s essential to detect and isolate these attempts before they spread and do more damage. The key elements of a detection system include:</td>
<td>Since no system is foolproof, airlines have to develop a methodology for responding quickly to an attack in order to limit reputational damage. And they need to use all details of the attack to enhance prevention.</td>
</tr>
<tr>
<td>• The critical role of boards of directors</td>
<td>• Monitoring network and IT systems</td>
<td>A good reaction plan includes:</td>
</tr>
<tr>
<td>• A proactive approach that includes knowledge of global threats—current and prospective, people and places</td>
<td>• Protecting customer and operational data</td>
<td>• Notifying customers and other stakeholders as soon as possible and managing press stories</td>
</tr>
<tr>
<td>• Expanding and formalizing industry standards</td>
<td>• Understanding and dealing with insider threats</td>
<td>• Collecting forensic data to identify security weaknesses</td>
</tr>
<tr>
<td>• Dealing with risks from supply chain, parts, and third-party vendors</td>
<td></td>
<td>• Minimizing damage caused by security breaches</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Closing the loop by using new information to improve prevention methods</td>
</tr>
</tbody>
</table>
Adlen LOUKIL, Ph.D
CEO, Resys-consultants

Advisory, Audit and Training –
Information Security, Business Continuity &
Risk Management

GSM: 0021698208872 – contact@resys-consultants.com
www.resys-consultants.com