Cyber Security: Airport risk and liability

Jean-Michel Fobe  Adrian Cioranu
Airport cybersecurity concerns

Infamous Hacker Creates Skyjack To Hunt, Hack, And Control Other Drones

Cyber attack led to Bristol Airport blank screens

Cyberattack claims multiple airports in Vietnam

Russian Hackers Attacked U.S. Aviation as Part of Breaches

Turkish hacker group says it was behind airport cyber attack
Why have aviation cybersecurity standards?
Why have aviation cybersecurity standards?
Why have aviation cybersecurity standards?

Cyber-threats and concerns are increasing everywhere, including aviation
Aviation is a system-of-systems with many stakeholders
To respond, all parts need to improve their security and resilience

• **Goal is safety, security and trust in aviation**

**BUT**, there is little common understanding of ‘how much is enough’

• Regulation is generally lagging the threat and should not over-specify
• Cannot rely alone on safety standards, but also cannot forget safety

**Therefore, existing, new and emerging standards play a key role**

• Supporting regulation
• Establishing good practice
• Defining and judging trust in others
Aviation cybersecurity is everyone’s responsibility

Who to trust?
Who is liable if there is a cyber-attack?
## Benefits of cybersecurity standards

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides a baseline for measurement and good practice</td>
<td></td>
</tr>
<tr>
<td>Enables your organisation to communicate your security approach and security status with partners</td>
<td>strengthen collective cybersecurity across aviation</td>
</tr>
<tr>
<td>Establishes a consistent (and usually iterative) approach</td>
<td>efficient and effective</td>
</tr>
<tr>
<td>Achieves regulatory compliance when MoC</td>
<td>legally operate</td>
</tr>
<tr>
<td>Encourages interoperability and cooperation</td>
<td></td>
</tr>
<tr>
<td>Creates market demands</td>
<td>reduces supply chain risk</td>
</tr>
</tbody>
</table>

MCGILL UNIVERSITY/PEOPIL CONFERENCE DUBLIN 19-20
OCTOBER 2018
2013 PWC cross-sector research


>1000 standards relating to cyber security in some form globally

• 89% were cross-sector
• 67% focus on organisational cyber security
• 3% focus on people cyber security

Only 25% of organisations invest in full implementation of at least one standard
1 in 4 then invest in external certification

1st main barrier to cyber security standards is that they are too expensive

ISO 27001 was the most common standard being implemented
Aviation cybersecurity standards landscape

Aviation-specific

General / Cross-sector

And more!

Global, regional and national players!
Aviation cybersecurity standards landscape... is complex

Changing regulatory environment: ICAO, Regional & National

• Regulation should point to cyber standards more than it does at the moment

• E.g. airworthiness regs will reference ED-202A and ED-203A (CS 25.13xx)

Landscape features some aviation-specific and many cross-sector cyber standards

• Aviation specific: ED-20x and EN 16495

• Cross-sector: eg ISO 27000 series and NIST

• Lots of guidance too: ICAO Manuals, ECAC Doc 30

• Landscape is evolving quickly: is it quick enough compared to the threats?

Big challenge for standard-making organisations to ensure:

• Completeness

• Consistency / coherency / harmonisation

• Timeliness
**Future developments**

**ED-205 – Security certification/declaration of ATM/ANS systems**
- In draft and expected to be published mid/late-2018
- A security method for ground ATM systems/services analogous to airworthiness certification

**EN 16495 - Info security for orgs supporting civil aviation operations**
- Revision expected in 2019?
- Alignment to ISO 27002:2013 controls, plus controls for each trust level

**ECAC Doc 30 - Chapter 14 – Cyber Threats To Civil Aviation**
- Ongoing updates, including domain specific advice

Expect **ED-201, ED-202A** and **ED-204** to be revised in 2019 and 2020
Plus WG-72 to develop Guidance on Security Event Management
1. Apply the principles of cybersecurity in the airport domain, working with other aviation actors (airlines, ANSPs, ground handlers, etc)

2. Select an appropriate standard, or set of standards, to adopt to:
   1. Manage cyber-risk (operational, safety, financial, reputational, etc)
   2. Comply with regulatory requirements

3. Undertake audits and other forms of assurance to have confidence, and instil trust in others

4. Include Cybersecurity risks in your Insurance Portfolio
WHAT is Cyber Liability Coverage?

Cyber liability insurance covers financial losses that result from data breaches and other cyber events

- First party coverage (e.g. damage to your company's electronic data files caused by a hacker)
- Third party coverage (e.g. claims against your firm by people who have been injured as a result of your actions or failure to act)

Losses Covered

- Loss or damage to electronic data
- Loss of income or extra expenses
- Cyber extorsion losses
- Notification costs
- Damage to reputation
- Network security liability
- Network privacy liability
- Electronic media liability
- Errors and omission liability
- Cyber terrorism liability
Be prepared!

THANK YOU