STAR 021 V1 – January 2016	Cyber Security (and the mitigation of threats)

Introduction

Almost every facet of business within the global aviation industry connects through technology, ranging from basic email systems to sophisticated on-board aircraft computer technology. The industry (airlines and ANSP's in particular) are constantly looking to improve both the flow of data and increase operational efficiency through the introduction of computer systems, and their integration to optimise the management of their networks. The number of software systems, connectivity and data entry points is increasing constantly, with systems and processes becoming more convenient, efficient and integrated, but are consequently increasingly vulnerable to cyber threat. For airlines to improve identification of the various cyber threats and ultimately to help in risk assessment and threat mitigation development, the reporting, sharing and understanding of information is essential.

Identifying and understanding the threat

The first challenge for an organisation when implementing Cyber security measures is to understand that there are three overarching common impacts of a malicious Cyber-attack that can threaten an airlines safety, security and IT system:

- Confidentiality (information that is classed as personal, financial or operational)
- Data Integrity (the insertion, modification or removal of data from a system)
- System/Data Availability (the attacker is able to present barriers to accessing the data)

Each of the above 'impacts' can then be further disseminated into six specific threats that can have a negative impact on an airline and/or their operation:

- Airport and Airline websites
- Airport and Airline staff databases
- Airline Booking Systems
- Aircraft Electronic Systems
- Air Traffic Management Systems
- Data Service Providers

It is also important that the appropriate departments within an airline are tasked with recognising and mitigating the threat – it is the responsibility of CEO's to task IT, Safety and Security departments to collaborate on cyber security.

Airport and Airline websites

There has been a large increase in the number of reported cases regarding the hacking of airport websites, for both malicious and vulnerability testing purposes. With regards to the latter, in November 2015 a UK airport had its website attacked by a hacker who wanted to test the websites vulnerability. As well as getting into the site, the hacker was able to obtain names and email addresses from a database. Although a spokesman for the airport stressed that the physical security had not been compromised, the concern is how this incident has highlighted the ease it could be for an individual who may want to hack a website for malicious purposes. A hacker could not only access confidential information, but also upload onto the website a specific/inflammatory political message or

even insinuate a bomb threat, resulting in the temporary evacuation of the airport etc.

Airline and Airport staff databases

These systems can be best described as 'soft targets', meaning that although sensitive data could be acquired, the safety implications are somewhat limited. Such information in these databases will primarily contain flight planning and crew information, as well as the personal details of staff members (e.g. security clearance, address, telephone, age) – personal information but not necessarily critical to safety.

Airline Booking Systems

Another 'soft target' where personal data relating to passengers is held in a confidential system. This data could include addresses and the financial details relating to how the flight was paid. Such information could be extracted by a hacker and used for financial gain, or to check the dates when a specific passenger was away and their home left vacant.

Of greater concern is the potential for a terrorist organisation (with the necessary hacking skills) to 'place' an individual on a flight as though they were a normal passenger. This individual could be a potential hijacker or have an alternative malicious intent.

Aircraft Electronic Systems

There has been much speculation in the media concerning the feasibility of a cyber-attack on an aircraft with the hacker being able to 'take control' of the on-board systems (avionics). There have been worrying reports of hackers who have claimed they were able to gain access to the avionics systems via the passenger in-flight entertainment (IFE) system and then be able to manipulate certain flight controls.
On certain aircraft, the IFE system provides audio and video entertainment for passengers through a monitor embedded in either an armrest, seat back or the ceiling. They can also display an animated map showing the flight route and the plane's speed and progress across the map. A connection between the avionics system and the IFE does exist, but there is a caveat in that the connection should allow for one-way data communication only.
Avionics systems are designed with built-in restrictions programmed into the software which are coded in such a way to reject any in-coming communication. In addition avionics systems are designed according to strict standards and undergo extensive code review and testing to ensure that nothing externally should be allowed to interfere with the system. Therefore at this time the ability to take control of an aircraft flight controls via the IFE system is not (yet) considered viable.

Air Traffic Management Systems

In order for flying to remain the fastest and one of the safest methods of transport, complex **air traffic management** (ATM) systems are required. These systems ensure that aircraft are not only guided safely through the sky, but also that the airspace is managed correctly to accommodate the ever-changing needs of air traffic.

If a hacker with malicious intent undertook a cyber-attack into an ATM system, the consequences of such actions could result in any number of serious safety events, including an airprox, runway conflict and deviation into unauthorised airspace. There has been a worrying increase in the number of reported incidents where hackers have been able to temporarily take over air traffic control transmissions and given pilots bogus commands. Fortunately in all those reported cases the pilots were able to ascertain that the directions given them were false.

Data Service Providers

These are organisations that provide their customer airlines with a full flight briefing service and or Departure Control Service (DCS). Such services may include either some or all of the following; the provision of computer flight plans, load and balance information, en-route and surface weather statistics, aircraft performance data, runway obstacle data and the latest Notices to Airmen (NOTAMs) pertinent to a particular route.

With such critical data contained within a computer flight planning system, a hacker with malicious intent could cause both the service provider and the airline, serious disruption, financial penalties and in extreme cases (depending on the nature of the data) an air safety incident/accident. For example, a computer flight plan factors in hundreds of variables, from weather conditions, to the expected take-off weight of the plane, to various air traffic control requirements, with the ultimate goal of reducing fuel consumption and minimising the risk of mid-air collisions. A simple (innocent) software bug would cause disruption, whereas the malicious removal or editing of data will result in far serious consequences. An aircraft could inadvertently be flown off course, in-correct take-off weights could result in a runway excursion or collision with an obstacle on climb out, and even a NOTAM could be hacked to provide the airline with incorrect information.

Addressing the cyber-security challenges

As one of the most complex and integrated systems of information and communications technology in the world, the global aviation system is an attractive target for a large-scale cyber-attack, or for a targeted attack on some of its most vital elements. While the industry cannot eliminate cyber risk, it must manage it. This is achievable, but will require a deep collaboration between authorities, industries and the academic world through an effective information sharing program that will leverage the collective power of the key players in the aviation industry.

In July 2015 the ICB (Industry Consultation Body) published a Position Paper on the Regulatory Response to ATM Cyber-Security. The paper states that a common and robust understanding of cyber-risks is vital to inform policy and regulatory decisions on appropriate responses. Risk tolerances, risk containment and the potential cost of specific responses also need to be better understood. In addition, the European Commission has developed a general Cyber-Security Strategy for the European Union setting out key roles and responsibilities and emphasising information sharing and coordination.

References and further information

- The IATA Aviation **Cyber-Security** Toolkit (and accompanying video), which provides tools & guidance for implementing a robust **cyber security** management system, can be located via the following IATA weblink: http://www.iata.org/publications/Pages/cyber-security.aspx

- In addition, the **IATA Security Group (SEG)** assists the Operations Committee (OPC) in all matters relating to the optimization of security measures to enable secure and efficient air transport: http://www.iata.org/whatwedo/workgroups/Pages/secwg.aspx

- **ENISA (European Network and Information Security Agency)**. ENISA is the EU's response to the cyber security issues of the European Union: https://www.enisa.europa.eu

- **The EU Cyber Defence Policy Framework** has been developed to assist in cyber-defence aspects of the EU Cyber-Security Strategy:

http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf