Airport Security*
Focus on Cyber Security

Nevo Barchad
Nevo.barchad@mfa.gov.il
Monaco, 1 June 2015

*Basic Assumptions

* The airline industry relies on computer systems extensively in its ground and flight operations

* Some systems are directly relevant to the safety of aircraft in flight, others are operationally important, and many directly impact the service, reputation and financial health of the industry


Exit

Basic Assumptions

- As IT systems become increasingly interconnected and interdependent, and critical systems become reliant on technology, Cyber Security has become an increasing concern in civil aviation
- The aviation sector is one the critical infrastructure systems that is not only vulnerable to physical threats, but also cyber threats, especially with the increased use of Bring Your Own Device (BYOD) at airports.

Basic Assumptions

- Cyber-security incidents are dramatically increasing year-on-year across the full spectrum of international trade
- Due to their visibility, disruption of the essential operations of airlines and airports could feasibly be the subject of a cyber-attack by cyber terrorists
- Cyber attacks will come from many sources and will have a range of possible targets, including civilian, commercial and military systems to damage critical services

Basic Assumptions

* Airport infrastructure supports many different operations that are critical for the efficiency and effectiveness of the air transport system
* Unfortunately, not all airports have implemented cyber-security systems that would protect and control those operations and all related features
* It means that even though many may have security measures in place, cyber terrorists may consider this as a perfect opportunity to attack the airports in many different ways

* ***It is usually said that there are types of security incident:***

* Natural Disaster
* Malicious Attack (External Source)
* Internal Attack
* Malfunction and Unintentional Human Error

* We only discuss attacks

Malicious attacks

- Malicious attacks are taking place all around the world almost every minute
- The targets vary from banking systems to e-mail servers
- In terms of airports, the most ‘desirable’ exposed parts could be public wireless hotspots; the baggage systems; main airport websites, and so on

Malicious attacks

* Just by virtue of the system itself, airports are particularly vulnerable to internal and external cyber threats and attacks from criminals, terrorists, or foreign actors.
* Apart from the traditional IT infrastructure such as the email and the Internet, several potential targets for cyber attacks exist within the realm of internal airport operations:
  * Access control and perimeter intrusion systems,
  * eEnabled aircraft systems,
  * Radar systems,
  * Ground radar,
  * Network-enabled baggage systems,
  * Wireless and wired network systems,
  * Supervisory Control and Data Acquisition (SCADA)-type ICSs.

* Beyond physical security at airports, cyber threats to the internal airport operations are emerging to be a primary concern especially with the increasing use of mobile applications and mobile hardware
* Even small airports are heavily dependent on networked computer systems for daily operations and are therefore vulnerable to cyber threats

* Malicious attacks

* In recent years, iPhones, iPads, Androids, and Tablets are a common sight in workplaces. This trend is also catching up at airports where not only the airport users, but even the airport personnel wish to bring their own devices into the workplace.
* However, if these devices interact with enterprise systems (such as e-mail and VPN access) they can potentially be used secretly gather confidential information or introduce viruses.

*Malicious attacks

* Airports typically rely on SCADA-type industrial control systems for utilities, baggage systems, and business processes such as facility management.
* Due to their limited or lack of internet access, SCADA-type systems may appear to be more secure, but they too are vulnerable to cyber threats

* Malicious attacks

* If a member of the airport staff destroys airport data, leaks sensitive information, or in a worst-case scenario, harms the systems intentionally

* Internal Attack

Why is it a desirable target for Terrorists?

- *Air transport industry is one of the targets likely to be selected by cyber terrorists*
- *Incidents may result in long-term implications for any type of airport – big or small*
- Loss of operations for any period of time would be crucial
- The same goes for reduced throughput of, for example, Hold Baggage Systems, which would lead to chaos from the passenger's side, and operational productivity would drastically drop

Why is it a desirable target for Terrorists?

- Moreover, the leakage or destruction of data does not sound convincing – sensitive information may reach third parties, which could be disastrous not only for the airport, but also for the whole of the aviation sector

- Airports as sign of governance being the gates to the country

Preparing for the worst

* There are many activities ongoing in from different institutions and bodies aiming at spreading awareness of cyber-attacks and how to protect businesses

* In 2013, for example, the European Commission released a policy document called Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace that invites industries to take actions at the national level in order to protect their business and to have harmonised cyber-security measures among all Member State airports in the EU

*So, what can be done?

* Furthermore, the European Civil Aviation Conference (ECAC) has a Study Group on Cyber Threats to Civil Aviation that considers recent developments in cyber-security and a cyber-threats, building a framework for establishing best practices for reducing cyber-attacks on critical aviation information systems (CIAS)

* So, what can be done?

So, what can be done?

- If we look at the US, the Transportation Research Board (TRB) is a part of the National Academies of Science that is aiming to develop Airport Cyber-security Best Practices

- The research team asks airports to share their experience, knowledge and concerns about cyber-security issues

* Firstly, it is important to recognize the cyber-risk and threat, and then it would be easier to establish a cyber-security strategy, objectives, vision, and mission
* Secondly, promotion of cyber-security awareness would be effective. In particular, industries should reflect on ways to make CEOs and Boards more accountable for ensuring adequate cyber-security measures

* *How airports can prepare?*

How airports can prepare?

- The first step could be training on cyber-security to all relevant staff, and a dialogue at all levels of airport management

- Furthermore, airports should regularly test their own systems through the use of external audits, penetration testing, and regular examination of the airport's websites

* *Security is a matter of economics*
* *Security should be composed of layers of defenses*
* *Absolute security does not exist*

* How airports can prepare?

* The importance of increased global cooperation and sustained commitment to implementing effective air traveler and border security controls, including against cyber threats
* Israel has some of the world leading companies in that field and is collaborating with like minded countries on a regular basis

* *How airports can prepare?*

*Global Cooperation

* Israel had joint seminars and workshops with like-minded countries on airport security

* Since 2012 Israel we include in the seminars a component of Cyber Threats

* Moreover, airports should be encouraged to share their experience with other airports and national and international organizations by spreading the word through conferences, meetings, and so on

* *How airports can prepare?*

* engagement and collaboration between the aviation industry and Government agencies is critical to supporting effective air traveler and border security
* The exchange of information such as advance passenger details, biometric information, and watchlist data, reinforces international good practices and supports good air traveler and border security

* Recommendations

* The number of global air travelers is expected to double from the current three billion per year to six billion by 2030, which can produce even larger threat if steps toward are not taken in the immediate future

* Recommendations

* There is absolutely no guarantee that cyber-attacks will not happen, but if – or rather when – they happen, the time it takes to recognise, analyse and respond to an incident will limit the damage and lower the cost of recovery to an airport

* The consequences can cost billions, but it is not only about the money: trust and reputation of the airport would be significantly harmed as well

*To conclude:

Thank you!*

Nevo Barchad

Nevo.barchad@mfa.gov.il