Aviation Security

Emerging Threats from Cyber Security in Aviation – Challenges and Mitigations

ABSTRACT

Security threats to civil aviation operations have become more sophisticated and challenging to deal with. One that is emerging and arguably even more complicated and sophisticated to manage is cyber-attack. Today, the global civil aviation community is relying on computer-based and information technology (IT) systems for their daily frontline and backroom operations. This reliance will continue to grow as new and modern airports are developed, new aircraft introduced into service and stakeholders seek to meet the growing demand of the more IT-savvy passengers with new passenger facilitation processes using digital and IT-based systems. Global civil aviation operations will certainly need to keep up with economic changes, and the use of more computer-based and IT systems will be a key driver of innovation and efficiency, including systems to enhance safety and security. This paper looks at some of the challenges and possible ways to address the concern of cyber security threats confronting the global civil aviation community.

THE AUTHOR

Mr Bernard Lim is Director (International Relations and Security) with the Ministry of Transport, Singapore. His key responsibilities include formulating and managing policy matters concerning international relations, transport security and transport emergency preparedness in Singapore. He is currently Chairman of the International Civil Aviation Organization (ICAO) Aviation Security Panel and Vice-chairman of the Asia-Pacific Economic Co-operation Aviation Security Experts Sub-Group. He had also led the ICAO Aviation Security Panel Working Group that developed the Comprehensive Aviation Security Strategy (2011 - 2016).

Prior to this, Mr Lim had held various positions in areas such as Airport Management and Ground Operations, Air Transport and Air Services Negotiations, International Relations, Aviation Security and Emergency Preparedness at the Civil Aviation Authority of Singapore.

Mr Lim holds a Master's Degree in Public Administration from the University of Liverpool, UK. He was trained in crisis management at the Emergency Planning College in York, UK, and in Leadership at the John F Kennedy School of Government, Harvard University, US.

Bernard Lim
Ministry of Transport, Singapore

INTRODUCTION

Despite the multitude of measures and investments made in enhancing security of civil aviation operations worldwide, aviation security remains a critical area of focus amongst all stakeholders. Since the terrorist attacks of 11 September 2001 in the US, there have been many more incidents that had followed thereafter, including the threat from liquid explosives in 2006, the "underwear bomb" in 2009, the attempt to destroy aircraft using improvised explosive devices hidden in printer cartridges in 2010, and the attacks at Moscow's Domodedovo Airport in 2011 and in Sofia, Bulgaria, in 2012, just to name a few. These incidents demonstrate that even though many new security Standards and Recommended Practices (SARPs) have been introduced under Annex 17 (Security) to the Convention on International Civil Aviation (ICAO, 2013), and despite the implementation of many new security measures by States and stakeholders, terrorists continue to look for new ways to carry out attacks on civil aviation operations to achieve their goals. Amidst all the efforts to deal with new and emerging aviation security threats, one major security challenge which the civil aviation community ought to quickly focus attention on is the threat from cyber-attacks.

GROWING RELIANCE ON COMPUTER-BASED AND IT SYSTEMS

Arguably, threats to civil aviation operations from cyber-attacks are not new. The use of computer-based systems in almost every aspect of civil aviation operations – ranging from sophisticated air navigation systems, on-board aircraft control and communications systems, airport ground systems including flight information and security screening, to simply inventory and day-to-day office data management systems – have been going on for many years now. Similarly, cyber threats such as computer viruses and more malicious deliberate attacks on computer systems by hackers and other adversaries are not new occurrences. With the continued growth of the global civil aviation industry, the increasing number of air travellers, development of new, larger and more modern airports as well as the introduction of new and more sophisticated aircraft, there will certainly be greater use of IT as well as more advanced computer-based systems in all aspects of civil aviation operations. This is also augmented by the drive towards achieving greater efficiency, reduction in the use of manpower, and greater use of IT to reduce cost and increase synergies between and amongst stakeholders. Many airports and airlines are also introducing more efficient ways for passenger facilitation, such as using mobile devices (e.g. Personal Digital Assistants) for electronic ticketing, check-in and immigration clearance. These innovative measures definitely widen the digital interface between airlines and airport

systems to a very large extent for the expanding number of passengers and airport users. Today, there is tremendous dependency on computer-based and IT systems in the entire architecture of a State's civil aviation system and this dependency will only continue to grow.

To compound the challenge, cyber security breaches or threats could range from opportunistic exploitation of innocent mistakes made by personnel operating the IT systems, mischief makers seeking the thrill of causing interference, inconvenience and nuisance to entities, to calculated and pre-meditated malicious attacks to cripple the operations of a civil aviation service provider or organisation that can disrupt operations and even threaten lives of innocent passengers, crew and ground personnel. With terrorists becoming more sophisticated and equally *au fait* with the use of computer-based and IT systems, cyber security is certainly the next frontier of threats and challenges to civil aviation operations.

In recent years, there have been a number of incidents that had been allegedly attributed to cyber-attacks which demonstrated that vulnerabilities in the civil aviation system to cyber security threats certainly exist and must be urgently addressed. These include:

- An attack on the internet in 2006 that forced the US Federal Aviation Administration (FAA) to shut down some of its air traffic control (ATC) systems in Alaska;
- The crash of Spanair flight 5022, a McDonnell Douglas MD82, just after take-off in Madrid-Barajas Airport on 20 August 2008, killing 154 people, where the Civil Aviation Accident and Incident Investigation Commission of Spain reported that the crash occurred because the central computer system used for monitoring technical problems on board the aircraft was infected with malware;
- An attack on an FAA computer in February 2009 where hackers obtained access to personal information on 48,000 past and present FAA employees;
- A cyber-attack that led to the shutdown of the passport control systems at the departure terminals at Istanbul Atatürk and Sabiha Gökçen airports in July 2013, causing many flights to be delayed; and
- An apparent cyber-attack that possibly involved malicious hacking and phishing targeted at 75 airports in the USA in 2013.

These are just some incidents that have been attributed to deliberate cyber-attacks against civil aviation operations. There are certainly many more, including those that are targeted at critical civil aviation systems and infrastructures that could lead to catastrophic consequences if left unchecked.

EFFORTS TAKEN TO ADDRESS CYBER SECURITY THREATS

The serious threats posed by cyber-attacks have certainly been well-recognised by many stakeholders in the global civil aviation community. Many efforts have been embarked upon

and more are being pursued to address these concerns – by regulators, airlines, airports, aircraft manufacturers, air traffic service providers, industry associations and ICAO.

Efforts Pursued by ICAO

ICAO, which is a United Nations specialised agency governing international civil aviation, has recognised the serious challenges posed by cyber security threats to civil aviation operations. In September 2012, delegates at the ICAO High-level Conference on Aviation Security requested that ICAO further address emerging aviation security issues including cyber threats. Following that, in October 2012 at the 12th ICAO Air Navigation Conference, where cyber security was discussed and recognised as a major concern, the cyber security task force was formed to evaluate the extent of the problem and draw up a global cyber security architecture that would include contributions from the industry. In that same year, Annex 17 (Security) to the Convention on International Civil Aviation, which lays down the security SARPs which ICAO Contracting States have to comply with, was amended to require that air traffic service providers establish and implement security provisions to meet the requirements of the national civil aviation security programme of that State. A new Recommended Practice was also introduced by the ICAO in Annex 17 (ICAO, 2013) stating that "*Each Contracting State should develop measures in order to protect information and communication technology systems used for civil aviation purposes from interference that may jeopardise the safety of civil aviation*". New guidance materials are being developed in support of these new SARPs.

The ICAO Aviation Security Panel (AVSEC Panel), which is made up of a group of experts tasked by the ICAO Council to look at aviation security threats and issues, and to develop recommendations for the Council to consider on aviation security policies, SARPS and other approaches, has also been actively looking at the threats posed by cyber security. At its 25th meeting in March 2014, the ICAO AVSEC Panel deliberated on a number of issues concerning cyber security threats. These include:

- An assessment provided by the ICAO AVSEC Panel's Threat and Risk Working Group on the risk posed by cyber-attacks against IT-based Air Traffic Management (ATM) systems, and encouraged further work on the matter, in collaboration with other stakeholders, to better address the evolving nature of the threat. The Working Group will expand its scope of work to look at other areas of cyber security threats and risks that can affect the civil aviation system and will report its assessments to the AVSEC Panel when ready;
- A discussion on the challenges of cyber security with other relevant organisations, such as the Civil Air Navigation Services Organisation, where the ICAO AVSEC Panel emphasised the need for all stakeholders to also look at cyber security threats beyond just ATM systems. These should include airport operations systems, airport security systems, airline systems, air navigation systems and others;

- A discussion on the merits for States to define responsibilities on cyber security management for aviation security in the National Civil Aviation Security Programme (NCASP), such as the tasks of the appropriate authority for aviation security; the civil aviation authority, airport operator, airlines, air traffic services providers, ground handling agents, security companies and other agencies involved in civil aviation operations;
- Encouraging States to develop an aviation security cyber security management plan. Such plans should include policies, approaches and, where possible, measures to address cyber security threats and attacks that could lead to acts of unlawful interference in civil aviation operations. The plan should also include incident management and business continuity; and
- Recommending that the ICAO AVSEC Panel work together with other relevant ICAO panels, external expert bodies such as standards authorities and the aviation and aircraft industries, to develop best practices and guidance on protecting aviation against cyber-attacks.

EFFORTS PURSUED BY OTHER ENTITIES

ICAO is not the only body that has been actively looking at developing standards, approaches and measures to address the threat from cyber security to civil aviation operations. A number of States have also been working on cyber security protection and mitigation plans to safeguard their critical civil aviation systems from cyber-attacks. Many airports and airlines have also been implementing measures to protect their IT systems and infrastructure from cyber-attacks, and continue to do so with new and more advanced technology being introduced to raise operational efficiency in their operations.

In support of the efforts by the airlines, the International Air Transport Association (IATA) has given due recognition to the threat that cyber security poses to airline operations worldwide. In line with its vision "*To assist airlines in developing a robust cyber security strategy and to drive coordination of global efforts in addressing cyber threats to civil aviation*", IATA has instituted a three-pronged strategy to address the cyber security threat. This strategy "*includes work to understand, define and assess the threats and risk of cyber-attack, advocacy for appropriate regulation and mechanisms for increased cooperation throughout the industry and with and between Governments*". To further supplement this effort, a first version of a toolkit to assist airlines to better understand and define the risks of cyber security threats was developed in 2013. This toolkit (IATA, 2014) contains, among others, guidance material for setting up a cyber security management system which would help airlines to assess risk.

In June 2013, the International Federation of Airline Pilots Association (IFALPA) issued a paper (IFALPA, 2013) that articulated the threat of cyber security attacks against aircraft, ground and other critical facilities and infrastructure supporting civil aviation operations. The paper also suggested a number of ways to address such threats. These include measures that can be taken to enhance the security of an entity's computer software and hardware – including

data protection, access control, physical separation of sensitive systems, training of flight crew, governance and control, protection of air traffic services and aircraft design and operation.

Aircraft manufacturers have also been actively working to protect aircraft on-board computer, navigation and other systems from possible cyber attacks and infiltration. Aside from security features to protect these systems, they are also working closely with aircraft certification authorities to ensure that cyber security concerns are adequately addressed. For instance, in November 2013, FAA issued special conditions to Boeing on the security features for the B777-200, B777-300, and B777-300ER series airplanes (FAA, 2013a). FAA is also working with Airbus on a set of special conditions for the A350-900 airplanes to include isolation or protection of the aircraft's electronic system security from unauthorised internal access (FAA, 2013b).

A number of professional organisations, academic and research institutions and others have also developed comprehensive studies and documents which could provide stakeholders with useful suggestions on how they could address cyber security challenges[1].

CHALLENGES AND NEXT STEPS AHEAD

Despite the multitude of efforts that have been undertaken, and more being pursued by various stakeholders, there still exists a number of issues and steps ahead that need to be addressed with regard to combating cyber security threats to civil aviation operations. While the road ahead may seem difficult to some, the rapidly changing global civil aviation landscape, fast pace of technological improvements and innovation, and the rising demand for operational efficiency, balanced with the critical needs to ensure safety and security, may leave stakeholders in the civil aviation community with little choice but to take up the challenge to deal with these sooner than later. Taking a few steps back, some fundamental questions need to be addressed first by States and their respective aviation security regulators on the issue of cyber security threats. These include:

- Which agency in the State is responsible for, and serves as the regulator of, cyber security issues and measures for its civil aviation community?
- Is the State's Appropriate Authority for Aviation Security adequately knowledgeable on cyber security threats to civil aviation systems and operations, the preventive and mitigation measures and possesses the ability to regulate and audit the various civil aviation stakeholders on compliance with Annex 17 SARPs as well as the cyber security requirements of the State's civil aviation security programmes?
- Are there relevant chapters or sections that lay down the critical requirements regarding cyber security protection and mitigation measures in the State's civil aviation security programmes (e.g. NCASP; Airport Security Programme; Operator Security Programme; National Civil Aviation Security Training Programme; National Civil Aviation Security Quality Control Programme)?

[1] For example, the American Institute of Aeronautics and Astronautics published a document entitled "A Framework for Aviation Cybersecurity" in August 2013.

- Does the State have in place, at the minimum, a national civil aviation cyber security policy? Going further, does the State have in place a national civil aviation cyber security plan? Is there an established structure within the State to bring together State agencies, industry and stakeholders in the civil aviation community to jointly address cyber security challenges and threats to civil aviation operations?

At the international level, some considerations could include:

- What further role can ICAO play to address cyber threats to civil aviation operations? These could include addressing cyber security challenges from a holistic civil aviation perspective and exploring further collaborations with other specialised agencies, while bearing in mind the need for keeping up facilitation in tandem with security.
- Are there further efforts that ICAO, States and stakeholders can take to enhance international collaboration and cooperation to address cyber threats to civil aviation operations?
- What can civil aviation stakeholders – aircraft manufacturers, airport operators, airlines, ground handling agencies, cargo and freight operators, in-flight catering companies, fuel companies, etc, do at the international level to collaboratively deal with cyber security issues that they commonly face?

And at the stakeholder's level, some pertinent questions for consideration could include:

- From the whole civil aviation perspective, does each and every stakeholder and entity in the civil aviation community, both from the private and public sectors, down to the level of responsibility of the individual organisation, agree that they have a critical role to play in safeguarding against cyber security threats?
- At the minimum, does each stakeholder have a cyber security plan in place to protect the organisation's critical data, information management systems, hardware and infrastructure and control of access to its critical infrastructure including access to sensitive information, which, if compromised, can lead to serious security breach or other disastrous consequences?
- Does each stakeholder have an appointed officer, reporting to the Chief Executive Officer, designated as the person responsible for ensuring the security integrity of the organisation's IT systems, cyber security protective and mitigation measures, as well as measures for recovery of its operations and critical data in the event of a successful cyber-attack?
- Does that appointed officer responsible for ensuring the organisation's cyber security integrity possess adequate expertise and knowledge on the company's IT systems as well as the impact on the company's operations? Is that officer working alone or does he/she have a team of trained personnel to assist in various cyber security prevention and mitigation functions?

- Does each stakeholder have in place a system or process to report all cyber security incidents and attacks, including anomalies and suspicious activities, to the State's civil aviation authority? This would facilitate swift responses and assessments as such attacks could lead to further attacks or impact on ongoing civil aviation operations at the airport or the ATC centre.

These are just some questions that could be imperative and form the key starting point for stakeholders who may be facing challenges grappling with the issues and concerns posed by cyber security threats. There are certainly many more questions and details that would help entities understand the critical and fundamental issues that would be in their interest to give necessary attention to, as cyber security threats and attacks permeate borders and can come from anywhere and at any time.

Following are some suggested actions which States and civil aviation stakeholders can consider when addressing these threats to enhance the security of their operation:

- Raising awareness within the organisation, from the top level down to the shop floor, on the critical importance of guarding against cyber threats. This can help all levels of personnel to appreciate the challenges and complications they can face if there is a compromise to the organisation's cyber systems, and every person has a responsibility to help prevent such cyber-attacks from succeeding against their operations.
- Every entity to take ownership of their organisation's cyber security needs and undertake an assessment of the organisation's cyber security vulnerabilities and measures in place, to identify and understand the gaps where cyber-attacks could possibly occur. Cyber security should be treated as an organisational responsibility, just as the organisation would accord importance to human resources management, finance, operations, infrastructure and other core functions. By treating cyber security as a company hygiene factor, there would naturally be adequate senior management attention and focus on cyber security efforts and measures that can go a long way to protect the organisation's operations, and in turn, the wider civil aviation operations of the State.
- Develop a cyber security policy and plan within the organisation. Such a policy is of increasing importance as it will set the thrust and tone of how the organisation would address cyber security issues, and the attitude which the rank and file should adopt towards cyber security. A company cyber security plan is also of growing importance as entities become more reliant on IT, as well as on more sophisticated and integrated computer-based systems. Moreover, many of these systems may be interfaced with those of other agencies or even individuals, such as passengers, to facilitate the smooth delivery and functioning of the whole suite of civil aviation operations. Passengers and airline crew today can even plug their computer or

other IT gadgets into an aircraft's inflight entertainment and other systems, which can be an avenue of vulnerability if not properly secured or managed. Many stakeholders also obtain their IT systems from external suppliers and outsource the maintenance of these systems to third party operators. These are further weak links that need to be addressed.

- In addition to a company cyber security preventive and mitigation plan, it would be useful for stakeholders to develop a recovery plan. This is to address actions that need to be swiftly taken in the event of a successful cyber security attack or breach, where immediate isolation of the affected systems may be needed, or recovery actions activated to restore the IT system or the operations (e.g. Flight Information Display, security pre-board screening, check-in, passport control, baggage handling, etc.), to resume normally.
- All these go back to the State having in place relevant requirements and regulations for cyber security in its national civil aviation security programmes. It is also imperative that the State's regulator for aviation security possesses the necessary expertise and knowledge in aviation security, civil aviation operations and cyber security, in order to be able to establish practical and sensible regulations, and provide the proper oversight, audit and compliance framework to ensure that cyber security measures have been adequately undertaken to protect the State's civil aviation operations from cyber threats.
- Greater information sharing amongst stakeholders, including between regulators and industry, and amongst relevant organisations, should be encouraged, to identify common threats and challenges posed by cyber-attacks on the security of civil aviation operations, as well as the sharing of best practices to address these threats and concerns.

CONCLUSION

The aviation security landscape is fast changing and becoming more challenging with this new frontier of cyber threats. While many States and stakeholders in the global civil aviation community are aware of the seriousness and catastrophic consequences that can come about from cyber threats, many are still grappling with these challenges and are not necessarily ready or equipped to deal with such threats confronting them, at both the individual level and national system-wide level. However, the use of more advanced and sophisticated IT and computer-based systems in civil aviation operations will continue and expand even more in the future. This will percolate down to even the most basic functions such as data collection and processing, where heavy reliance on the security of IT systems will become critical. The cyber frontier is massive and there are numerous inroads which terrorists and malicious persons can use to conduct a cyber-attack on civil aviation services providers and critical infrastructure. Therefore, it is crucial that ICAO, States, international organisations and associations, and all civil aviation stakeholders, work to raise the level of awareness and recognition of the cyber security threat, and undertake actions, even if at an incremental pace, to protect and mitigate against cyber threats that can seriously impair and cripple the global civil aviation system.

References

FAA. (2013a). Docket No. FAA-2013-0958. Special Conditions: Boeing Model 777-200, -300, and -300ER Series Airplanes; Aircraft Electronic System Security Protection From Unauthorized Internal Access. Washington, DC. Federal Aviation Administration, US Department of Transportation.

FAA. (2013b). Docket No. FAA-2013-0910. Special Conditions: Airbus Model A350-900 Airplanes; Isolation or Protection of the Aircraft Electronic System Security From Unauthorized Internal Access. Washington, DC. Federal Aviation Administration, US Department of Transportation.

IATA. (2014). Statement on Cyber Security. Aviation and Border Security. Geneva. International Air Transport Association.

ICAO. (2013). Annex 17 to the Convention on International Civil Aviation – Security (9th Edn). Montreal. International Civil Aviation Organization.

IFALPA. (2013). Paper 14POS03. Cyber Threats: Who Controls your Aircraft. UK. The International Federation of Air Line Pilots' Associations.