Airport cyber resilience and managing supply chain risk

Dr Richard Piggin EngD CEng MIET MBCS

Introduction

Airports are in a competitive environment, seeking to enhance their appeal, improve their customer experience and innovate with digital transformation. Safety and security remain paramount and have converged, with cyber security becoming an increasing and enduring focus, given the increasing number of high-profile incidents and new regulation. The introduction of the European Network and Information Systems (NIS) Directive underlines the necessity for airports to actively manage cyber security risk to maintain services and ensure their rapid restoration in the event of a cyber security incident. Both airports and regulators have recognised the importance of managing critical supply chain risk is a collaborative responsibility, achieved with trusted partners to maintain cyber resilience.

Governance & cyber resilience

Cyber resilience involves more than security according to the World Economic Forum aviation cyber security study. It requires focus on protecting critical functions, not only assets (WEF, 2020). Airport CEOs and Directors are accustomed to being held accountable for airport performance. However, cyber security has often been considered the domain of IT technologists. It is not merely an IT issue; Operational Technology (OT) operates critical airport functions.

Cyber security is the responsibility of the entire airport organisation and effective cyber security relies upon the leadership and support of the airport's management team. Recent alerts, press coverage, social impact, legal cases, and regulatory intervention have demonstrated that CEOs and Directors will be held accountable for significant cyber security breaches. Organisations need to be employ recognized good practices to be resilient in the event of cyber incidents, and to avoid being deemed culpable.

Threats to airports and impact on operations

Cyber-attacks or compromises can disrupt airport operations and interfere with systems (ACI-RASC, 2019). It is essential that airports have a robust cyber security programme to maintain resilience. All businesses, including airports are at risk and can become victims; airports have been specifically targeted. The commercial, operational, and reputational impacts could be highly damaging (DfT, 2018). It is estimated that one hour of disruption in a large airport could cost more than €1 million at peak operating times (ACI, 2019). EASA estimated there are 1,000 cyber attacks each month on aviation systems worldwide (PA Consulting, 2018). In the UK 75% of large organisations identified and reported a cybersecurity incident in the last 12 months (DCMS, 2020). The ACI 2020 COVID-19 pandemic report indicated that 61.5% of airports had experienced targeted attacks. Respondents reported phishing (77%) malware (51%), and denial of service (21%) as the most common attacks (ACI, 2020).

Most cyber incidents are malicious (52%) according to IBM, the remainder being attributed to human error or system glitches. Many cyber security incidents often go unnoticed or unreported. The IBM breach survey (IBM, 2020) indicated the average time to identify and contain a breach took over 9 months (207 days to identify and 73 days to contain a breach). Costs mount significantly the longer this breach lifecycle takes to resolve. The airports trade association Airports Council International (ACI), highlighted potential impacts to airports from a cyber security incident in the Cybersecurity for Airport Executives guidance (ACI, 2019):

- **Operational disruption**—The loss of major systems required for airport operation. This may include passenger-facing systems such as flight information displays; airline check-in facilities; departure-control systems; and security systems, and baggage systems or operational control systems. In 2017 Ukraine's Boryspil International Airport lost access to its systems. including flight scheduling information due to the NotPetya malware (The Independent, 2017). A distributed denial of service (DDoS) attack targeted the Polish LOT airline in 2015. The carrier's IT systems were affected, grounding over 1,400 passengers for five hours at Warsaw's Frederic Chopin Airport (Reuters, 2015).
- **Economic impact**—Financial information theft or fraudulent transactions are common cyber security crimes and can have serious economic impacts. Operational disruption can also result in serious economic impact. The Maersk shipping company declared losses exceeding $300 million, when the NotPetya malware disrupted global shipping operations. Fedex's European TNT operations were also disrupted by NotPetya, estimated losses and recovery expenditure were expected to exceed $500 million (Piggin, 2018).
- **Reputational damage**—Loss of proprietary or sensitive information can often have an impact on an airport's business reputation and stakeholder trust. Cyber security incidents impacting operations are commonly reported in the press and rapidly circulated through social media. The loss of a USB memory stick by a Heathrow airport employee was widely reported in the press, following its discovery by a member of the public. The USB memory included sensitive information in the over 1,000 files, which were not encrypted or password protected (BBC, 2017; Mirror, 2017). San Francisco International Airport published a data breach notification indicating that some users of its websites may have been the victim of user login credentials during a cyber-attack in March 2020 (IAR, 2020).

- **Legal consequences**—Data protection and privacy laws require management of the security of all personal data and the retention of security information. Compromising this data can have legal consequences if the airport is found not to have adequate controls in place. Heathrow Airport was fined £120,000 for serious failings in its data protection practices for the loss of the USB stick and the data protection breach (ICO, 2018). The UK Information Commissioner's Office (ICO) fined Cathay Pacific Airways £500,000 for failing to protect the security of its customers' personal data. Poorly protected systems exposed customers' personal details, 111,578 of whom were from the UK, and approximately 9.4 million more worldwide.

  The ICO announced an intention to fine British Airways £183.39 million under General Data Protection Regulation (GDPR), for the breach of personal data of more than 400,000 customers and staff in 2018. The sanction was reduced to £20 million in 2020, following improvements to its security arrangements, and the regulator considering the economic impact of COVID-19 on their business and representations to the ICO. It is the largest penalty the ICO has issued to date.

  The NotPetya cyberattack in June 2017, regarded at the largest reported cyberattack in history, has highlighted the threat to unconnected and non-targeted organisations. A principal concern for organisations affected by cyber security incidents is the risk of management liability lawsuits (DAC Beachcroft, 2019). Cyber security follow-on class actions are increasing being brought against companies and their directors. Recent aviation examples include British Airways and EasyJet. Easyjet is facing a staggering £18 Billion claim (Covington, 2020).

The US National Security Agency (NSA) and the Cybersecurity & Infrastructure Security Agency (CISA, part of the US Department of Homeland Security) recently published an alert recommending critical infrastructure organisations take immediate actions to secure their operational technology assets (NSA and CISA, 2020). The alert describes the "perfect storm" of potential access to unsecured and vulnerable assets, the use of publicly available device/systems information, and extensive list of exploits deployable via widely available tools. These approaches are not technically advanced, but are considered to pose a serious threat due to the significant potential impact to critical assets.

The NSA and CISA alert provided details of recently observed cyber threat activities, which illustrate potential attack methodologies, and their impact upon operational technology:

Recently Observed Tactics, Techniques, and Procedures

- A highly targeted bespoke email (spear phishing) is used to launch malware on a victim's computer and obtain initial access to the organization's information technology (IT) network, before transitioning to OT systems.
- Deployment of commodity ransomware to encrypt data for impact on both IT and OT networks.
- Connecting to remotely accessible systems without user account or password authentication for initial access.
- Using common network protocols to communicate with devices and download modified programs.
- Use vendor engineering software and program downloads.
- Modifying device/system programs and configurations.

Impacts

- A loss of availability of the system.
- Partial loss of view for human operators, where equipment operators are unable to use operator displays to view performance or potentially interact with a system.
- Resulting in loss of productivity and revenue.
- Adversary manipulation of control and disruption to physical processes.

The potential consequences for airport operational technology are shown in Table 1

Table 1 Potential airport threat events that may impact operational technology based upon NIST SP 800-82 Rev 2 (Stouffer et al., 2015)

Threat event	Description
Malware on device/systems	Malicious software (e.g. Virus, Worm, Trojan, Ransomware) introduced onto the device or system
Denial of control action	Device/system operation disrupted by delaying or blocking the flow of information, denying device or system availability or the use of networks used to control device or system to the airport
System, application, configuration or software manipulation	Device, software or configuration settings modified producing unpredictable results
Spoofed device/system status information	False information sent to either to disguise unauthorized changes or to initiate inappropriate actions by airport staff
System functionality manipulation	Unauthorized changes made to embedded software, programmable instructions in airport systems, alarm thresholds changed, or unauthorized commands issued to devices, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of devices and functions, or even disabling airport equipment
Safety functionality modified	Safety-related functionality manipulated such that safety systems do not operate when needed; or perform incorrect control actions, potentially leading to employee or public harm or damage to airport equipment

Cyber risks also include:
Data exfiltration from systems connected to the equipment, even if protection measures are in place, and no other apparent routes for connectivity (eg. Ethernet, Wireless, Wifi, USB, removable media).
Network breach – network exploitation/reconnaissance, delivery of tools to facilitate exploitation, with potentially no indications that it has taken place.
Network attack – delivery of malware, exfiltration of data, compromise of systems, unauthorized operation, spoofing of data/systems, and other actions. Attacks include ransomware, that prevents access to systems or destructive malware, that deletes data and can render computers unserviceable. Potential denial of service of equipment and airport or unintended operation with potential safety consequences for staff, public and physical assets.
Connectivity to other systems such as security cameras, HVAC, building management systems, baggage handling systems, airport infrastructure and a compromise of those systems and therefore risk of compromise to other systems, and ultimately, the airport.

The increasing reliance upon digital technologies and the integration of Internet of Things (IoT) devices will increase potential exposure to cyber risk. Airport digital technologies now reach beyond the traditional administrative activities to critical airport functions (ACI, 2018).

Critical infrastructure & EU Network and Information Systems (NIS) Directive

The NIS Directive has concentrated airport executive's attention on cyber security and resilience, with a potential maximum €20 million penalty for operators of essential services. The Directive aligns with similar and emerging international regulation for Critical Infrastructure Protection (Wilson Center, 2017). It places an onus on executive boards to manage airport cyber risk and apply judgement. Not merely, or naively demand compliance from the supply chain. Operators of essential services need to implement 'appropriate and proportionate security measures to manage risks.'

Airports will need to demonstrate cyber security capability and practices to protect critical services to avoid potential noncompliance before, and in the event of disruption. It demands identification of critical suppliers and collaborative management of shared cyber security risk (Piggin, 2018). The Directive creates four high level objectives:

- Appropriate organisational structures, policies, and processes to understand, assess and manage security risks.
- Proportionate security measures to protect essential services and systems.
- Capabilities to ensure defences remain effective and detect cyber security events.
- Capabilities to minimise the impacts of a cyber security incident on the delivery of essential services including the restoration of those services where necessary.

The UK National Cyber Security Centre (NCSC), part of GCHQ, has produced comprehensive guidance for NIS Directive implementation and self-assessment (NCSC, 2020). The NCSC Cyber Assessment Framework (CAF) principles are acknowledged good practice, and define a set of top-level outcomes, which describe good cyber security. The NCSC has referenced existing guidance, which aligns with established cyber security frameworks, including the US National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF). Both the NCSC CAF and NIST CSF include guidance for managing supply chain risk.

Managing cyber security risk

Airport cyber security governance must extend to the supply chain, and proactively engage and collaborate with critical suppliers. Cyber security needs to be addressed from inception, beginning at the design and conceptual phase, progressing through every stage of system design, development and operation until the system is retired. Airports should consider suppliers that have a similar commitment to cyber security.

According to ACI (ACI, 2019), supply chain risk assessment practices should include the following activities:

- Supply chain risk management processes managed by airport stakeholders.
- Suppliers and third-party partners providing services and systems are identified, risk assessed and prioritized.
- Procurement measures meet cyber security programme objectives in accordance with the cyber security risk management plan.
- Suppliers and third parties are routinely assessed and evaluated to ensure they are meeting obligations.

Quality control measures or cyber security assurance activities should be applied to suppliers and service providers. These include system configuration, physical access, authentication, system interconnectivity, malware detection and routine vulnerability patching requirements (ACI-RASC, 2019).

Recommendations

Airports should follow published guidance for supply chain risk management and collaborate early with key suppliers to assess cyber security maturity. Trusted suppliers should demonstrate a mature approach to cyber security. They will have a robust product cyber security programme that addresses the entire security lifecycle and supports the shared responsibilities for both the airport and supplier, including cyber security assurance activities. Suitable critical suppliers will have invested in cyber security expertise and utilise a recognised security approach, aligned to global cyber security frameworks. Key indicators will include an established governance structure for product cyber security, a secure product architecture with product testing and risk management; performed by competent personnel actively managing the entire cyber security lifecycle.

References

ACI-RASC (2019) *Guidance Document on Cybersecurity for Airport Security Managers*. Hong Kong.

ACI (2019) *Cybersecurity for Airport Executives Handbook*. Montreal.

ACI (2020) *Airport Cybersecurity COVID 19 Survey Report*. Montreal: Airports Council International.

ACI (2018) *Airport Digital Transformation Best Practice*. Montreal: Airports Council International.

BBC (2017) *Heathrow probe after 'security files found on USB stick' - BBC News*. Available at: https://www.bbc.co.uk/news/uk-41792995 (Accessed: 11 October 2020).

Covington (2020) *EasyJet Latest Firm to Face UK Data Breach 'Class Action' - Lexology*., *Lexlology* Available at: https://www.lexology.com/library/detail.aspx?g=190a991b-b7d0-410e-bd16-20c9587ba6ff (Accessed: 11 October 2020).

DAC Beachcroft (2019) *FedEx securities class action following the NotPetya cyberattack*. Available at: https://www.dacbeachcroft.com/en/gb/articles/2019/november/fedex-securities-class-action-following-the-notpetya-cyberattack-implications-for-do-insurance/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration (Accessed: 11 October 2020).

DCMS (2020) *Cyber Security Breaches Survey 2020*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf (Accessed: 18 September 2020).

DfT (2018) *Aviation Cyber Security Strategy*. Available at: www.gov.uk/dftGeneralenquiries:https://forms.dft.gov.uk (Accessed: 14 September 2020).

IAR (2020) *San Francisco International Airport victim of cyber-attack in March 2020*., *International Airport Review* Available at: https://www.internationalairportreview.com/news/115026/san-francisco-airport-cyber-attack/ (Accessed: 11 October 2020).

IBM (2020) *Cost of Data Breach Report 2020*. Armonk.

ICO (2018) '*Heathrow Airport Limited fined £120,000 for serious failings in its data protection practices*', Information Commissioner's Office (ICO) Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/heathrow-airport-limited-fined-120-000-for-serious-failings-in-its-data-protection-practices/ (Accessed: 11 October 2020).

Mirror (2017) *Terror threat as Heathrow Airport security files found dumped in the street - Mirror Online*. Available at: https://www.mirror.co.uk/news/uk-news/terror-threat-heathrow-airport-security-11428132 (Accessed: 11 October 2020).

NCSC (2020) *NCSC CAF guidance*. Available at: https://www.ncsc.gov.uk/collection/caf (Accessed: 18 September 2020).

NSA and CISA (2020) '*Cybersecurity Advisory NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems*', (July), pp. 1–5.

PA Consulting (2018) *Overcome the Silent Threat: Building cyber resilience in airports*. London.

Piggin, R. (2018) 'Securing Critical Services', *ITNOW*, 60(2), pp. 58–61. Available at: 10.1093/itnow/bwy057 (Accessed: 1 June 2018).

Reuters (2015) *Polish airline, hit by cyber attack, says all carriers are at risk*. Available at: https://www.reuters.com/article/us-poland-lot-cybercrime-idUSKBN0P21DC20150622 (Accessed: 11 October 2020).

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. and Hahn, A. (2015) *Guide to Industrial Control Systems (ICS) Security*. Gaithersburg, MD: National Institute of Standards and Technology. Available at: 10.6028/NIST.SP.800-82r2 (Accessed: 27 March 2018).

The Independent (2017) *Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers*., *The Independent* Available at: https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-computers-wannacry-ransomware-a7810471.html (Accessed: 11 October 2020).

WEF (2020) *Advancing Cyber Resilience in Aviation: An Industry Analysis*. Available at: www.weforum.org (Accessed: 23 September 2020).

Wilson Center (2017) *Digital Futures Project*. Available at: https://www.wilsoncenter.org/sites/default/files/media/documents/publication/approach_to_critical_infrastructure_protection.pdf (Accessed: 23 September 2020).