Client Alert

pillsbury

Privacy, Data Security &
Information Use

Global Sourcing Cybersecurity Task Force

August 24, 2015

Cybersecurity and the Aviation Sector: Recent Incidents Highlight Unique Risks

By Mike Pierides, Brian E. Finch, Rafi Azim-Khan and Steven P. Farmer

Given the range of threats and the catastrophic impact an attack could have on an airline, strategizing to reduce the risk of breaches and implementing plans to deal with them once they occur should be prioritized at board level. We consider some recent examples of cyber incidents faced by the industry.

Whilst cybersecurity has ranked (or should have ranked) increasingly high on many boards' agendas for some time now, the risks associated with an attack on an airline places them in somewhat of a unique position. In particular, should an airline suffer a cybersecurity attack, this might not solely result in the loss of data, whether that be customer records, financial details of customers or sensitive details about company revenue; rather it could well impact an airline's core operations, with cyberattacks having the potential to seriously disrupt and endanger the safety of flights.

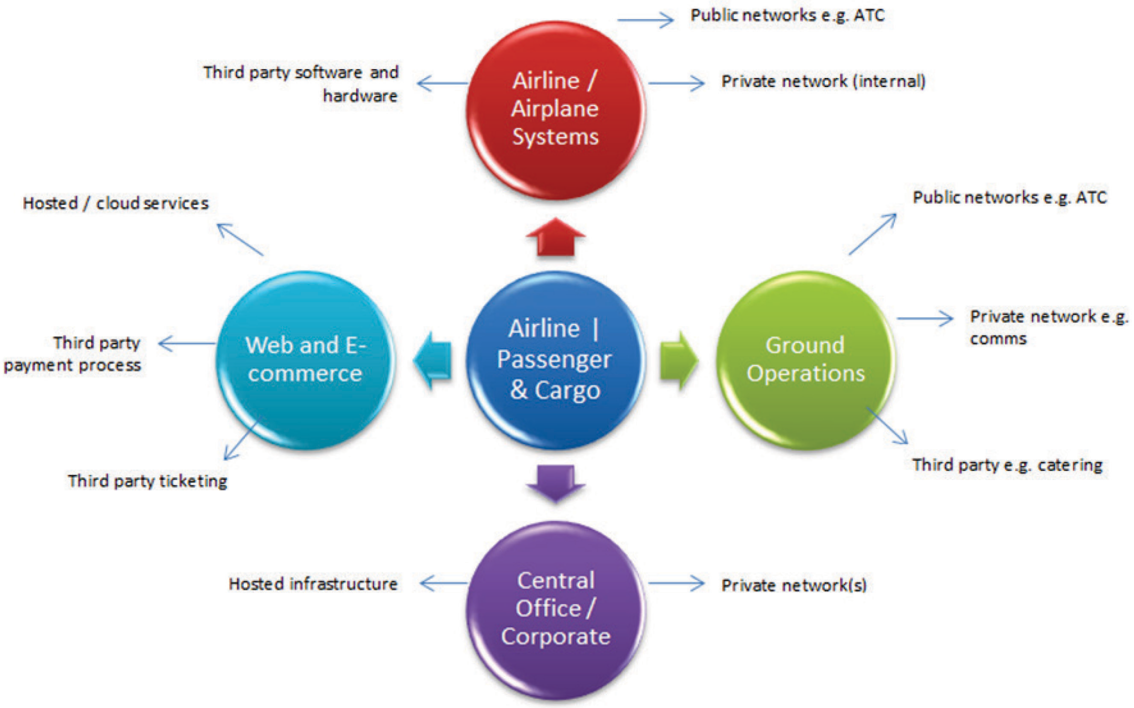
Recent incidents and unique challenges faced by airlines

Two recent examples highlight the fact that those who wish to harm an airline need not necessarily pass through a departure lounge any longer:

(i) On June 21, LOT Polish Airlines had its flight operations system hacked, resulting in disruption or cancellation of 22 flights. While there is little public information, and indeed there are some conflicting reports as to whether this was an actual cyber security attack, it is reported to have been a Distributed Denial of Service (DDoS) attack on a private network responsible for issuing flight plans, showing the scope for penetration into the inner workings of an airline's IT estate; and

(ii) In April, American security researcher Chris Roberts claims to have accessed flight-critical controls through the in-flight entertainment system (though this is rebutted by Boeing).

A specific challenge for airlines which heightens their cybersecurity risk is the incredibly diverse nature of their business in terms of geography, business lines (passenger and cargo), complex public and private systems (see diagram below), and significant interfaces with other bodies in the industry. This is an environment with many access points and potential points of weakness. As members of Boeing's cybersecurity team have said, “pervasive and instantaneous network connectivity, once limited to IT environments, is now a part of the global aviation culture.”


Public networks e.g. ATC
Third party software and hardware
Airline / Airplane Systems
Private network (internal)
Hosted / cloud services
Public networks e.g. ATC
Third party payment process
Web and E-commerce
Airline | Passenger & Cargo
Ground Operations
Private network e.g. comms
Third party ticketing
Third party e.g. catering
Hosted infrastructure
Central Office / Corporate
Private network(s)

Regulations and standards in the sector

As the industry responds to these threats, there is currently no uniform benchmark standard(s) or regulation for bodies to aim toward. At a regulatory level, there are some principles of general application primarily in relation to the security of data (for example the risk-based approach to security envisaged by the European Economic Area’s Data Protection Directive); however they are of very general and high level application, and not specific to the industry. Aviation regulators and industry officials are in fact pressing for greater collaboration between governments and airlines to protect the industry from cyber breaches, as was evidenced by the briefing of European ministers by the head of the European Aviation Safety Agency in early July.

From a standards perspective, there are a variety of initiatives: Aircraft manufacturers are providing guidance on best practice. Trade association IATA is developing a security toolkit. Airlines are taking unilateral action, e.g. the “bug bounties” of frequent flyer miles purportedly being offered by airlines such as United to buy the assistance of those who have uncovered weaknesses in the company’s IT infrastructure. But these only go so far, and none of these initiatives offer a silver bullet in light of the risks posed.

This is a game of cat and mouse against those looking to breach security, and the risks presented were possibly best summarized by Adrian Kubicki, spokesperson for LOT in the wake of their DDoS incident, who stated that “[LOT is using] state-of-the-art computer systems, so [this event] could potentially be a threat to others in the industry.”

Specific activities

For each individual airline, the key is a harmonized, coordinated approach across the entire company, including all geographies, business units and the supply chain.

A federated or autonomous organization in terms of purchasing standards and contract terms, technology standards, and internal governance or policies will struggle to create an effective approach to cyber security. The weakest link in the organization will open up the rest to potential attack.

Specific coordinated activities across an airline should include:

- Central determination of technology standards, policies and procedures to be applied across the IT environment, to be applied to own-hosted environment, and any third-party-hosted systems. As part of this, contract risk should be transferred to third party suppliers as appropriate.
- Full audit of existing IT systems with assessment of coverage gaps and overlap, but also compliance with the new standards. Poor interoperability between both hardware and software leads not only to customer service weaknesses, but also security vulnerabilities.
- Review of supply chain arrangements across the organization, and, again, contract risk should be transferred to third party suppliers as appropriate.
- Establishment of internal governance to proactively and reactively address cybersecurity issues, from the c-executive (whether this is a Chief Risk Officer or another officer tasked with this responsibility) down through the organization without gaps or competing committees or initiatives.
- Focus on employee and consultant arrangements, including training, screening and vetting, and authorization and access permissions. (Humans are typically the weakest link in any cybersecurity chain.)
- If an available avenue, have legal and compliance teams work proactively with local regulator(s) in order to help shape and drive the legislative framework that is inevitably being developed in this space.

Careful planning and preparations upfront, will not only limit damage should a breach occur but can also help avoid or minimize any regulatory sanctions, be good for an airline's reputation, and vastly improve a passenger's trust and confidence.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Mike Pierides (bio)
London
+44.20.7847.9559
mike.pierides@pillsburylaw.com

Rafi Azim-Khan (bio)
London
+44.20.7847.9519
rafi@pillsburylaw.com

Brian E. Finch (bio)
Washington, DC
+1.202.663.8062
brian.finch@pillsburylaw.com

Steven P. Farmer (bio)
London
+44.20.7847.9526
steven.farmer@pillsburylaw.com

About Pillsbury Winthrop Shaw Pittman LLP

Pillsbury is a full-service law firm with an industry focus on energy & natural resources, financial services including financial institutions, real estate & construction, and technology. Based in the world's major financial, technology and energy centers, Pillsbury counsels clients on global business, regulatory and litigation matters. We work in multidisciplinary teams that allow us to understand our clients' objectives, anticipate trends, and bring a 360-degree perspective to complex business and legal issues—helping clients to take greater advantage of new opportunities, meet and exceed their objectives, and better mitigate risk. This collaborative work style helps produce the results our clients seek.

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.