www.pwc.com/us/airlines

Aviation perspectives

2016 special report series: Cybersecurity and the airline industry

Part 1 of 4: Introduction

pwc

Cybersecurity has become an elevated risk that is among the most pressing issues affecting businesses. Today's cyber adversaries are more persistent, skilled, and technologically savvy than just a year ago, and leaders across all industries are taking notice. According to PwC's 2015 Global Airline CEO Survey, 85 percent of airline CEOs view cybersecurity as a significant risk, likely reflecting the highly sensitive nature of flight systems and passenger data.

In this edition of ***Aviation Perspectives****, we begin a four-part special report series that examines cybersecurity in the context of the airline industry. Following this 2016 introductory volume, we will analyze this issue in terms of prevention, detection, and reaction, and discuss actionable steps that airline executives can take to prepare for the evolving cyber threat environment.*

Online attacks are on the rise resulting in headline-grabbing stories. In the last few years, we've witnessed data breaches across multiple industries including banking, retail, health insurance, and online-only businesses. The financial impact alone is staggering. The cost of data breaches globally could reach $2 trillion by 2019.[1] Another study estimates that 2014 cybercrime losses cost businesses about $400 billion annually.[2]

Inevitably, cyber threats will continue to grow in number, cost, and sophistication. Consider the greatly expanded use of cloud and mobile devices. Businesses are embracing these tools to connect their internal staff and operations. They're also accelerating usage to connect externally—with strategic partners, customers, and a multitude of other third parties. These efforts are serving to enhance efficiencies, collaborations, and competitiveness. But along with these benefits, new vulnerabilities have emerged. Mobile devices create more entry points for hackers by dispersing data. The cloud, where data are aggregated, makes data more accessible. And these sources of risk are continuing to expand—quickly. To mitigate the threats, companies will need to reassess all facets of their business and establish internal protocols to effectively manage them.

Furthermore, as businesses aggregate and analyze more data on customers and processes, the data become increasingly valuable and a more attractive target for hackers. This double-edged sword applies to technology as well. While improved technology allows businesses to better understand and target their customers, advances in technology also provide hackers with more sophisticated technology with which to perpetrate attacks.

1 ZDNet, *Data breaches to cost global economy $2 trillion by 2019*, May 12, 2015. www.zdnet.com/article/data-breaches-to-cost-2-trillion-by-2019/

2 CRN Magazine, *The Total Global Cost Of Cybercrime? $400 Billion A Year And Growing*, June 9, 2014, http://www.crn.com/news/security/300073063/the-total-global-cost-of-cybercrime-400-billion-a-year-and-growing.htm

For the airline industry, cybersecurity risk is top of mind. According to our survey, 85 percent of airline CEOs expressed concern about this risk versus 61 percent of CEOs in other industries, a difference of 24 percentage points.[3] As in other industries, airlines are concerned with the theft of sensitive customer or company data. But an added threat for airlines is that technology is being used to improve the connectivity of flight operations systems with ground crews and air traffic systems. While this enhanced communication and integration is essential to the improvement of financial and operational performance,[4] it does provide more opportunities for those seeking to exploit these advances. So as airlines increasingly adopt advanced technologies, they must also upgrade security procedures to allow for safe innovation.

Overall, security procedures to date have been effective, safely integrating the many technological advances introduced to aircraft and airlines. Yet the industry continues to see major technological advances that contribute to the complexity of protecting data and assets. Two of these are tablet-based electronic flight bags (EFBs) and the installation of in-flight entertainment and Wi-Fi connectivity systems (IFEC).

EFBs are particularly popular with pilots as they have taken the place of heavy binders that pilots used to carry on-board. Yet a recent survey revealed that many airlines do not have a targeted plan in place to safeguard the security of EFBs.[5]

On-board IFEC systems are proliferating. Currently, they are physically segregated from cockpit systems. Nevertheless, these systems greatly increase the number of connections, vendors, and technologies involved, which in turn creates more hacking opportunities.

The threats posed by EFBs and IFECs need to be managed holistically, with airlines closely cooperating with other carriers, hardware and software providers, aircraft OEMs, and other industry stakeholders.

Another potential cyber issue for the airline industry is the Federal Aviation Administration's (FAA) modernization of air traffic control, notably the Next Generation Air Transportation System or NextGen. The current system is 40 years old and relies on radar, which provides limited connectivity. NextGen seeks to improve network efficiency by using GPS (global positioning system) that is software-based and connected to the Internet. While it's widely accepted that this transition is needed to modernize our air traffic control systems, the General Accounting Office has voiced concern that implementing a system with Internet connectivity brings with it greater threats to security.[6]

"…enhanced communication and integration is essential to the improvement of financial and operational performance, [yet] it does provide more opportunities…to exploit these advances."

3 PwC, 2015 Global airline CEO survey, *Getting clear of the clouds: Will the upward trajectory continue?* Dec. 2015. http://www.pwc.com/us/en/industrial-products/publications/assets/pwc_2015_global_airline_ceo_survey.pdf

4 PwC, Tailwinds: *2014 airline industry trends - The connected airline*. http://www.pwc.com/us/en/industrial-products/publications/assets/pwc-tailwinds-the-connected-airline.pdf

5 CSCSS, *Airlines and Hacking*, August 14, 2015, http://cscss.org/CS1/index.php/2015/08/14/216/

6 GCN, Cyber risks inherent in NextGen transition, GAO warns, April 27, 2015. https://gcn.com/articles/2015/04/27/faa-nextgen-cybersecurity.aspx

As real-time aircraft connectivity continues to evolve, providing information where and when it's needed to optimize airline operations and the customer experience,[7] it not only increases the number of opportunities for attacks, it potentially makes them more damaging. The industry is making significant investments and taking important steps to address cybersecurity, calling for increased oversight from boards of directors as well as third-party providers. The FAA has "convened a private meeting" to examine the security of aircraft systems,[8] which at the very least is an acknowledgement of the need for industry-wide approaches and standards. Tony Tyler, the head of the International Air Transport Association, or IATA, has publicly stated that regulators have to work with airlines to develop a global security system that adopts "an end-to-end risk-based approach."[9] IATA's position is that the industry can effectively deal with most attacks by focusing efforts on prioritizing and allocating resources to protect the airlines' most valuable assets.

In the interim, without any uniform industry standards in place, each airline has to consider how to reduce the risk of a cyber attack and how to deal with one when it happens. Regardless of how a cybersecurity strategy is formulated, the airline's board has to support the strategy and ensure that it is coordinated across all departments in the organization.[10]

A cybersecurity strategy includes methods to prevent, detect, and react to attacks as well as a mechanism for capturing learnings. Feedback collected at each stage should be incorporated into the overall security program to make attacks more difficult to execute successfully. While prevention methods are not foolproof, an airline's first security goal is to try and stop attacks from occurring, both on the ground and in the air. Once an attack occurs, airlines must detect the attack as quickly as possible and isolate the intrusion. And then airlines have to react quickly and efficiently to minimize the damage and reduce the risk of future incidents. As we have seen in many industries, this involves extensive analysis of the potential vulnerabilities across an organization's internal operations, supply chain, and strategic partner network.

7 PwC, Tailwinds: *2014 airline industry trends - The connected airline*. http://www.pwc.com/us/en/industrial-products/publications/assets/pwc-tailwinds-the-connected-airline.pdf

8 JDA Journal, *Cybersecurity Threat To Aircraft Is Being Addressed By FAA And Panel*, July 1, 2015. http://Jdasolutions.aero/blog/aircraft-cybersecurity

9 IATA, *Remarks of Tony Tyler at the IATA 22nd AVSEC World in Istanbul*, November 5, 2013. http://www.iata.org/pressroom/speeches/Pages/2013-11-05-01.aspx

10 MRO Network, *Cyberattacks and the aviation sector: how can airlines best prepare?*, September 28, 2015. http://www.mro-network.com/guest-blog/2015/09/28/cyberattacks-and-aviation-sector-how-can-airlines-best-prepare

In the next three parts of this 2016 Aviation Perspectives series, we'll delve deeper into the measures airlines are taking to prevent, detect, and react to cyber threats and how these efforts might be strengthened. We'll use specific examples from outside and inside the industry to illustrate what is currently happening in the threat environment and the related potential impacts on the airlines. And, as with any rapidly evolving ecosystem, we'll examine emerging risks on the horizon, both probable and theoretical.

Part 2: **Prevention**

The first line of defense is to prevent attacks that can corrupt or destroy data and interrupt operations. We'll discuss key elements of attack prevention that include:

- The critical role of boards of directors
- A proactive approach that includes knowledge of global threats—current and prospective, people and places
- Expanding and formalizing industry standards
- Dealing with risks from supply chain, parts, and third-party vendors

Part 3: **Detection**

Even with the best prevention systems, determined hackers will get through. It's essential to detect and isolate these attempts before they spread and do more damage. The key elements of a detection system include:

- Monitoring network and IT systems
- Protecting customer and operational data
- Understanding and dealing with insider threats

Part 4: **Reaction**

Since no system is foolproof, airlines have to develop a methodology for responding quickly to an attack in order to limit reputational damage. And they need to use all details of the attack to enhance prevention. A good reaction plan includes:

- Notifying customers and other stakeholders as soon as possible and managing press stories
- Collecting forensic data to identify security weaknesses
- Minimizing damage caused by security breaches
- Closing the loop by using new information to improve prevention methods


LOW CLEARANCE
4.4m

Contacts

To have a deeper conversation about the subjects discussed in this report, please contact the following:

PwC airline specialists:

Jonathan Kletzel
US Transportation & Logistics Leader
+1 (312) 298 6869
jonathan.kletzel@pwc.com

Richard Wysong
US Transportation & Logistics Director
+1 (415) 498 5353
richard.wysong@pwc.com

Alexander T. Stillman
US Transportation & Logistics Director
+1 (202) 487 8086
alexander.t.stillman@pwc.com

Rajeet Mohan
US Transportation & Logistics Director
+1 (305) 375 6239
rajeet.mohan@pwc.com

PwC cybersecurity specialists:

Charles Beard
US Advisory Principal, Forensic Services
+1 (703) 918 3318
charles.e.beard@pwc.com

Mickey Roach
US Advisory Partner, IT Security
+1 (214) 756 1635
mickey.roach@pwc.com

Rik Boren
US Advisory Partner, Cybersecurity and Privacy
+1 (314) 206 8899
rik.boren@pwc.com

Darren Orf
US Advisory Director, Cybersecurity and Privacy
+1 (312) 298 5072
darren.c.orf@pwc.com

Editorial contributor

Gloria Gerstein

For general inquiries, contact

Diana Garsia
US Transportation & Logistics Marketing Senior Manager
+1 (973) 236 7264
diana.t.garsia@pwc.com