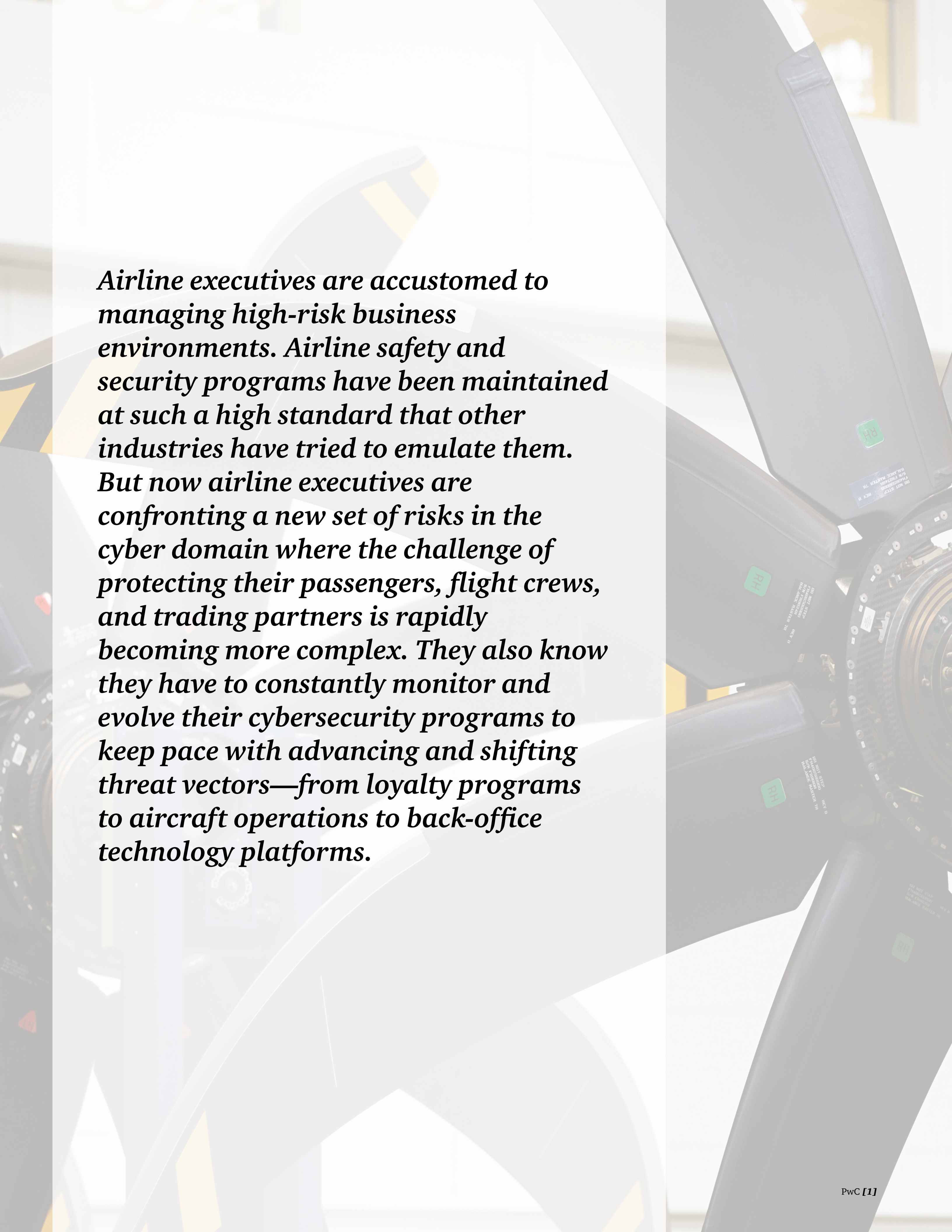
www.pwc.com/us/airlines

Aviation perspectives

2016 special report series: Cybersecurity and the airline industry

Part 2 of 4: Prevention

pwc



Airline executives are accustomed to managing high-risk business environments. Airline safety and security programs have been maintained at such a high standard that other industries have tried to emulate them. But now airline executives are confronting a new set of risks in the cyber domain where the challenge of protecting their passengers, flight crews, and trading partners is rapidly becoming more complex. They also know they have to constantly monitor and evolve their cybersecurity programs to keep pace with advancing and shifting threat vectors—from loyalty programs to aircraft operations to back-office technology platforms.

Unscheduled disruptions of transport carrier operations can have a substantive economic impact on third parties and national economies. Preventing disruptions caused by cyber events is increasingly a primary focus for those involved in global air transport. In the United States, transportation companies in general, and air carriers in particular, are expected to have cybersecurity programs that align with the National Institute of Standards and Technology (NIST) standards. Implementing proactive, reasonable measures to prevent cyber events in the air transport arena extends beyond the carrier and requires a concerted effort by original equipment manufacturers (OEMs), maintenance, repair, and overhaul (MRO) providers, air traffic controllers, airport authorities and operators, and third-party suppliers that provide catering, IT services, hardware, and other critical inputs to an airline.

A key decision for airlines is determining what "reasonable security" means for the organization and how much to invest in prevention. What is reasonable for a regional carrier operating a single model fleet of regional jets built by one OEM and flying to 32 gates per day is vastly different from a global carrier operating a mixed fleet from multiple OEMs and flying to hundreds of global destinations, including high cyber and physical security threat locations. A good way to consider trade-offs for prevention is to think about horizontal breadth of protection and vertical depth of preparedness. For example, if an airline invests too much in the latest prevention tools (vertical depth), it risks lagging in the horizontal investment to protect the breadth of the airline's value chain—interactions required with OEMs, MROs, and global distribution systems (GDS). Conversely, carriers that underinvest in vertical preparedness risk having a security portfolio that lacks tools and techniques to detect and prevent more sophisticated attacks.

What constitutes an effective defense plan? There are several key elements:

Oversight at the board level and building a security culture

A cybersecurity program has to rest on a risk-based framework that addresses risks across the airline including back-office IT, maintenance, operations, and consumer-facing systems because failure in one area can affect others. Management, employees, and the board must become more cyber aware as breaches can occur as a result of small lapses in procedure. But security awareness training is not enough. Airlines need to incorporate cyber awareness into the security culture, embedding cybersecurity into the organizational fabric. Below are specific examples of the roles various functions need to play:

- Procurement: looks for the counterfeit parts that may have come unwittingly from providers
- Maintenance: considers the security maturity of MRO partners and potential points of ingress;
- Operations: considers enhanced digital security measures needed to fly safely to high-risk destinations;
- Marketing: examines the value of consumer information and guards against identity theft and exploitation of awards programs;
- Information technology: modernizes infrastructure and implements security monitoring and remediation protocols that establish resiliency for flight operations;
- Management: sets the tone at the top and appropriately communicates to the broader enterprise and its trading partners;
- Board: ensures operational cyber risk is put in context of other carrier risks and is properly resourced.

> *"Airlines need to incorporate cyber awareness into the safety culture, embedding cybersecurity into the organizational fabric."*

Proactive approach that sets priorities

Since it's too expensive to protect all assets from all threats, airlines need to prioritize—assets, threats, and threat perpetrators. On assets, they have to recognize their protection obligations, identify associated digital assets, and focus aggressively on protecting those assets most valuable and critical to the organization. On threats, airlines need to prioritize and categorize the kinds of threats they are facing, both those known currently and those projected to emerge over the next few years, and recognize the signs of an attack early on. On perpetrators, they need to look at the players that are most threatening, a list which can include nation states, organized crime, and terrorists.

Airlines cannot do this by themselves: the risks are too numerous and diverse—and constantly changing. They need to avail themselves of all existing tools, public and private, that can help mitigate risk.

In the United States, the NIST Cybersecurity Framework supports businesses in critical infrastructure industries including transportation. In addition, the Department of Homeland Security established the Critical Infrastructure Partnership Advisory Council (CIPAC) for aviation as a public-private partnership to address the cyber risks affecting the industry.

To augment this industry sector insight with carrier-specific threats, many airlines subscribe to threat intelligence services that inform them about the latest threats. Airlines then can model different scenarios to determine optimal prevention approaches. Real-time feeds from these services are fed into security operations procedures so they can be dealt with.

Many carriers are also harnessing the power of the cloud and big data to model and monitor evolving and new cybersecurity threats. Using these new technologies allows airlines to scale protection efforts across their organization and increase the sensitivity of their prevention programs. Additionally, some companies perform periodic penetration assessments. These are generally commissioned by senior management to evaluate the strength of security and monitoring procedures.

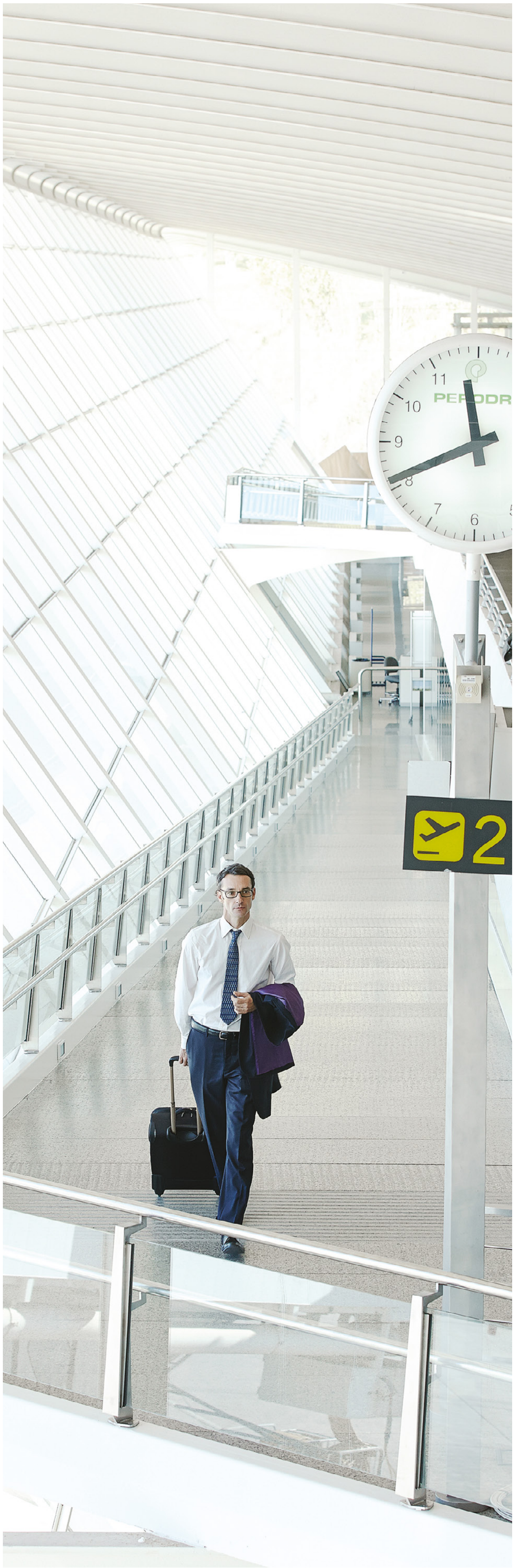
Support international standards

There are no international standards for cybersecurity design and testing, which is widely acknowledged to be an issue. The US, Europe, and the International Air Transport Association (IATA), a trade association of the world's airlines, have begun initiatives to address the lack of standards. Last year, the US Federal Aviation Administration, or FAA, established a new industry working group to provide guidance on how to improve cybersecurity on e-enabled aircraft.[1] The European Aviation Safety Agency (EASA) held a workshop to address cybersecurity. IATA has also called for better sharing of airline cyber threats among governments and airlines worldwide and asked governments around the world to take a more active stance in improving cybersecurity.[2]

Airlines can do their part by supporting efforts to build international standards. While industry associations establish standards, airline CISOs could form informal alliances to discuss leading practices in the industry and how best to implement those practices. These peer-to-peer interactions can lead to focused discussions on specific threat areas.

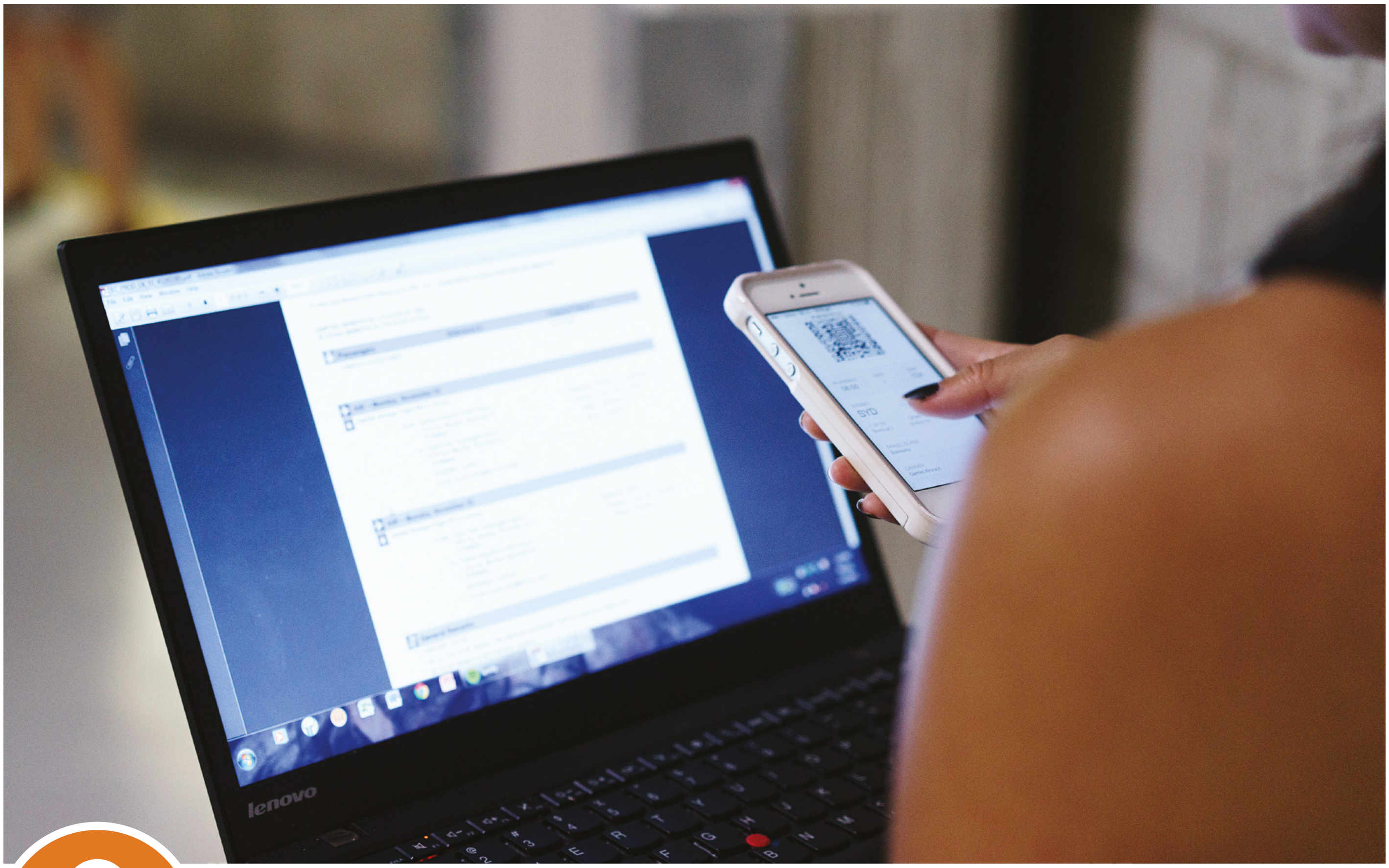
Address supply chain risks

It's critical that airlines and their external partners (such as OEMs, MROs, IFEC [in-flight entertainment and communications] providers) collaborate on threats and response techniques to share best practices to increase the knowledge base. But, in addition, airlines have to monitor partners' operations for potential security breaches and manage the access of users to different systems. In particular, smaller companies tend to have less stringent security protocols and invest less than their larger counterparts in security measures. To mitigate risk, airlines have to ensure their vendor contracts include audit clauses and specified testing procedures.



[1] https://www.runwaygirlnetwork.com/2015/02/12/faa-to-establish-aircraft-cyber-security-working-group/

[2] http://www.caa.gov.qa/content/iata-calls-better-sharing-airline-cyber-threats



Cybersecurity capabilities. Beyond these broad strategic approaches to cybersecurity, airlines need to consider the technologies and processes that can strengthen their programs to deal with today's threats. Some of those tools are described below:

Threat intelligence

Airlines must gather both external and internal threat intelligence from multiple sources including third-party vendors, subscription feeds, and agencies as well as system event and log information. This information can then be correlated and fed into a 24 x 7 x 365 security operations center (SOC) to help identify and prioritize threats.

It's also key that airlines get involved at an industry level so they can raise awareness of threats among colleagues. One such organization, the Aviation Information Sharing and Analysis Center (A-ISAC), helps constituents better prepare for and manage sector-specific threats, vulnerabilities, and incidents. Other organizations that can provide intelligence include federal agencies, such as the FBI and the Secret Service, and industry consortiums, such as ISACA (Information Systems Audit and Control Association) and CERTs (Community Emergency Readiness Teams).

Identity and access management

Identity and access management (IAM) is often overlooked as a legacy capability, yet it provides a suite of functionality that authenticates and authorizes employees, partners, and customers to access airline applications and systems. IAM systems may cover many functions: ecommerce, ticket purchase, loyalty redemption information, and concourse applications to generate boarding passes, and also enable collaboration between airlines and governmental agencies, such as the Department of Homeland Security, and communication with MRO partners.

There are a number of capabilities within IAM. One is privileged access management (PAM) that is meant to protect against the use of generic and shared IDs. The system includes capabilities for enforcing, controlling, and managing privileged access to systems; logging, monitoring, auditing, and certifying privileged access; and reporting violations.

Another variation is multifactor authentication (MFA), which has been adopted by leading airlines that have moved beyond a 'passwords only' approach. It requires more than one method of authentication from independent categories of credentials to verify a user's identity and is usually comprised of something you know (e.g., password), something you have (e.g., token) and something you are (e.g., biometric). MFAAs restrict access to an airline's Internet and employee portals as well as key enterprise systems.[3]

Adaptive authentication solutions add an additional layer of security. They assess the risk associated with each authentication attempt/transaction by requesting additional attributes that help to verify identity. With basic password authentication, systems are vulnerable to attackers exploiting credentials that were compromised elsewhere. In the airline industry, several carriers have been hit with millions of dollars in fraud related to unauthorized redemption of miles and points by rogue attackers. The full value of adaptive authentication comes from establishing normal behavioral patterns of users and populations and then detecting anomalies by applying contextual data about the user, endpoint, transaction, or asset to make a risk-based authorization decision (e.g., logging in from a new geographic location).

Data protection/encryption

Leading airlines use encryption and tokenization technologies to help protect customer and employee information, including payment cards, national IDs, passport numbers, and bank accounts. This is particularly critical in today's digital environment with widespread use of social media and online applications. One example of a dynamic regulatory environment recently, the European Commission proposed changes to its privacy laws to strengthen and unify data protection for individuals in the EU. It also addresses export of personal data outside the EU. More importantly, it stated that the penalties and fines for the most egregious violations could be up to four percent of an organization's revenue.

Design/application security

Leading airlines are embedding security requirements from the 'ground up' and not as an afterthought, starting with the design of secure applications and products. According to NIST, it is 6.5 times more expensive to find and address an application flaw in development than during design, 15 times more expensive during testing, and 100 times more expensive during production.

In the past, efforts may have been limited to regulated or commercial applications that were in scope for SOX 404 or the payment card industry (PCI). However, this left mission-critical operational systems for ground and aircraft operations as well as MROs and other third parties out of scope for security. The threat landscape that airlines face has moved beyond the theft of data such as payment cards and towards the operational resiliency and integrity of all systems. Furthermore, any products and services that are developed for the crew, ground operations, and customers must consider security as a key functional requirement in today's landscape.

Security awareness

Whether it's the tampering of concourse devices, activity within the cabin (e.g., plugging into USB ports), or corporate espionage, awareness is often the front-line defense against threats. All airline employees, not just the physical and information security departments, have to share in that awareness and understand their roles and responsibilities in preventing cyber attacks. A good analogy for the depth of cultural integration required is the way that environmental safety regulations have become ingrained in the factory culture. For example, workers understand they need to wear certain footwear on a production floor for safety reasons and would almost certainly stop someone from wearing open-toed sandals. In the factory, policy and heightened awareness have been woven into the fabric of the culture through tone at the top, organizational campaigns, and incentives as well as penalties.

A similar cultural commitment is needed on the cyber front. For example, phishing attacks are still one of the most effective attack vectors used by adversaries; they are very easy to exploit and can yield significant returns even if just one target takes the bait. In such an attack, an employee is targeted to open an email link, which then downloads malware that infects the IT environment of the entire organization. Recently, executives have been the target of these types of attack because of their access to sensitive data. It's easy to see how one unwitting employee or executive can lead to significant damage.

In the next part of this airline cybersecurity series, we'll look at ways airlines can detect an attack—even as it is happening. While prevention methods can deter many or even most attacks, there will invariably be some hackers that manage to circumvent or penetrate security systems. When an attack occurs, speed is of the essence. The earlier an attack is detected, the sooner the organization can muster its resources and contain any damage.

[3] https://www.secureauth.com/Company/News/December-2015/SecureAuth-Survey-Finds-66-of-Cybersecurity-Profes.aspx

www.pwc.com/us/airlines

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

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

PwC cybersecurity specialists:

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

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

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

Mir Kashifuddin
US Advisory Director, Cybersecurity and Privacy
+1 (214) 754 4537
mir.kashifuddin@pwc.com

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