McKinsey & Company

Travel, Transport & Logistics Practice

How airlines should manage IT failures and security breaches to improve operational stability

To face up to challenges stemming from digital innovation, airline executives should work to secure technology delivery, manage cyberrisk, and address costs, among other actions.

by Thomas Elsner, Christoph Fuchs, Benjamin Klein, and Wolf Richter

November 2019

More than four billion airline passengers will book flights this year, and they expect to reach their destination on time, safely, and securely. Airlines rely ever more on digital technology to manage everything from booking and in-flight entertainment to aircraft maintenance. Technology outages and cyberincidents around the world have demonstrated that even some of the largest airlines need to upgrade their IT and operational technology systems, including their technology architecture and underlying infrastructure, to reduce risk and build resiliency into their heavily digitized operating model.

In 2019, for example, the United Kingdom imposed a $230 million fine on a European airline for a 2018 breach caused by security vulnerabilities in its website. Multiple airlines have had problems with their ticketing systems and an important aviation-infrastructure system, causing delayed flights and passenger check-ins. In 2018, hackers penetrated unpatched servers and access controls of an Asian airline to steal the personal and travel data of as many as 9.4 million customers, including 860,000 passport numbers. In 2017, a European airline experienced a major IT failure, causing delays and cancellations for more than 1,000 flights. Exhibit 1 shows a snapshot of recent, publicly reported IT and cyberincidents in the airline industry.

Digital innovation exposes airlines to growing risk for IT outages and cyberattacks

While the basic concept of flying has not changed since the advent of aviation, the continuous digitization of processes like capacity planning, crew assignment, flight operations, and predictive maintenance expands airlines' digital footprints and introduces new technical challenges to their operating models. More airlines are moving to the public cloud, for example, to harness data analytics and optimize customer experience and operations. As airlines integrate a wider array of ecosystems, such as those facilitated by the International Air Transport Association New Distribution Capability Standard, to personalize their offerings further and exchange more granular information with partners, they may have less control over the security environment and become more prone to digital attacks.

Given the industry's low margins, airlines also continuously look for cost-cutting opportunities, including in IT. Many try to optimize vendor contracts for unit costs rather than acquire the agility or innovation required to evaluate new business concepts and respond quickly to new threats or opportunities. Even worse, many airlines lack elementary tools to evaluate or respond to cyberincidents—for example, documentation of central IT systems and networks or information that would help map customer-facing business processes to IT systems affected by an outage during an incident.

As cornerstones of public infrastructure and modern society, airlines are also exposed to a growing number of successful cyberattacks. The increasing attack surface stemming from digital innovation across the airline value chain combined with the sheer amount of personal customer data, financial data, and location data they possess has made airlines a hot target for cybercriminals. According to Identity Theft Resource Center statistics for the United States, despite a recent decline in the total number of data breaches to about 1.2 billion, the number of records exposed has grown by about 15 percent per year since 2005 to more than 447 million in 2018 (Exhibit 2).

Airlines are in a difficult position. They need to innovate quickly to keep pace with industry trends and maintain lucrative positions in the changing value chain, but many lack the means to do so. Therefore, many rely on patches and workarounds in their digital backbones, potentially increasing cyberrisk and driving up IT costs—along with reputational and regulatory costs—in the long run.

How airline leaders can meet the challenges

Given the gravity, complexity, and growing number of risks—in addition to the limits on human and

Exhibit 1

The airline industry has had several recent system outages and cyberattacks.

Outages and cyberattacks

● System outage ● Cyberattack

Human error

● **September 2010:**
Airline (AUSTRALIA)
Upgrade to the booking, check-in, and boarding systems resulted in 2 system failures in the first 3 months; hardware failure and subsequent system outage affected ~400 flights

● **September 2014:**
Airline (ASIA)
Phishing attack resulted in exposure of personal information of up to 750,000 members of frequent-flyer club; later investigation by airline confirmed theft of >4,000 customers' personal details

● **January 2019:**
Aircraft manufacturer
Company detected a cyberintrusion on its commercial-aircraft business-information system, resulting in unauthorized access to data and compromised professional-contact and IT-identification details of some employees

Applications

● **June 2015:**
Airline (EUROPE)
Distributed denial-of-service cyberattack grounded ~1,400 passengers

● **March 2019:**
Travel-technology company
Reservation-system outage delayed passenger check-ins of various major airlines

● **April 2019:**
Aviation-infrastructure-system provider
Outage of key system that provided weight-and-balance information needed to clear planes for takeoff delayed flights for multiple US airlines

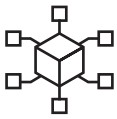
Data

● **July 2016:**
Airline (ASIA)
Website breach leaked names, dates of birth, and addresses of ~400,000 members of frequent-flyers club

● **June 2018:**
Airline (EUROPE)
Security incident tricked ~500,000 customers into exposing their log-in, credit-card, and itinerary information; airline was fined $230 million in July 2019

● **August 2018:**
Airline (AMERICA)
Undetected unusual log-in behavior in mobile app exposed data (including passport number, country of issuance, NEXUS number, gender, date of birth, and nationality) of up to 20,000 users, compromising sensitive user information

● **January 2019:**
Airline (ASIA)
Unauthorized access to personal data (including name, date of birth, passport number, and historical travel information) compromised sensitive user information of up to 9.4 million passengers



Infrastructure

● **July 2016:**
Airline (AMERICA)
Failed computer-network router disrupted airline's reservation system, leading to >2,300 canceled flights within 4 days

● **August 2016:**
Airline (AMERICA)
Global computer-system outage caused large-scale cancellations, resulting in flights grounded for 6 hours; 1 airline confirmed >1,000 of its flights affected

● **May 2017:**
Airline (EUROPE)
Major IT failure affected >1,000 flights

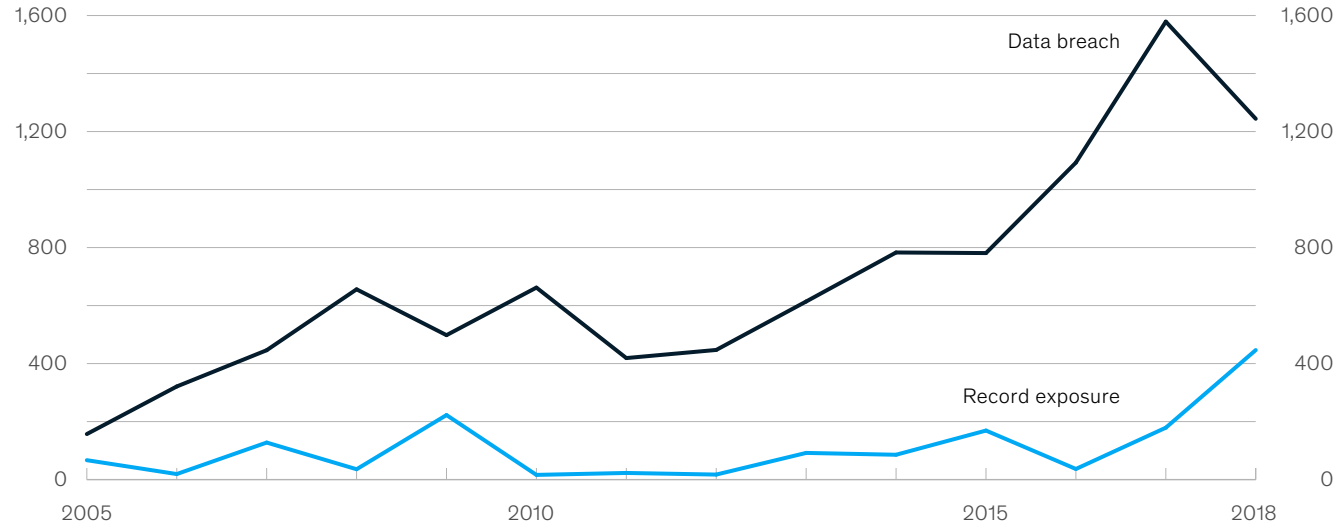
● **June 2017:**
Logistics company (EUROPE)
Cyberattack resulted in shutdown of multiple sites and business units

● **April 2019:**
Airline (AMERICA)
Global computer-system outage grounded flights for several hours, causing large-scale cancellations across several airlines

Exhibit 2

The exposure of passenger records to cyberattacks has increased.

Data breaches and record exposures in United States, 2005–18, million



Source: Identity Theft Resource Center; Statista

financial resources—that airlines face, airline executives need ways to set priorities and sequence their cybersecurity and digitization investments. Based on our experience in serving carriers around the world and leaders in industries from consumer lending to national defense, we recommend that senior teams step back and consider their overall situations from a business perspective. Digitization requires a powerful, reliable backbone that has security and resilience built in, not just what is available at the lowest possible cost. Airline executives should rethink their companies' approaches in three main areas: securing technology delivery, managing cyberrisk, and addressing costs.

Continue to get foundational protections in place and enable next-generation-technology delivery

An airline should build an IT architecture and IT operating model that best support its growth, digitization, and business model. Many of the airline industry's recent developments in digital passenger experience as well as optimized operations and maintenance processes rely on modern technology platforms and IT services. Without a modern IT infrastructure that serves as a platform to facilitate those digital services and processes, airlines risk falling behind in the race to attract new generations of travelers or to increase operational efficiencies further. It is therefore important to reconsider the current setup and find ways to modernize it. Many airlines will need to rebuild internal capabilities that they neglected during times of heavy outsourcing. A widespread example is the secure integration of cloud technology with existing networks, often involving a switch from a hub-and-spoke infrastructure to a distributed-infrastructure concept, where traditional perimeter-security models no longer work. In addition, airlines should strongly focus on continuing to get foundational protections in place.

Build security into digital products and processes and perform a detailed quantitative risk analysis

Cybersecurity should be central to every strategic decision and an essential component of every IT product in the organization. Cybersecurity initiatives should be prioritized based on business-risk scenarios. By looking across the business through a cybersecurity lens, airlines can transform their decision making and make wiser investments based on risk. Reviewing potential attack vectors from a risk perspective and evaluating the effectiveness of current cybersecurity activities could help identify areas that put the airline at risk but are not yet covered by running cyberactivities. Additionally, some in-flight cyberactivities might reduce risk in areas where the airline might not be exposed to significant threat.

Improve cost effectiveness

Airlines need to find ways to cover the rising costs of IT to meet innovation and cybersecurity requirements, help fund the modernization of the IT backbone, and lay the foundation for innovation. To generate true cost savings, the operating model needs to be adjusted. In the case of public cloud, standardizing and automating IT-infrastructure operations can significantly reduce costs. For example, automatic provisioning of ready-to-run environments for applications, fully defined in code, including all required security and network settings (without requiring manual interaction), reduces time to market while also ensuring cybersecurity. Defining functional platforms and driving standardization within and across those platforms also is a key enabler for "the platform play," an approach on how to structure IT to operate more like a tech company.

To keep airlines on track and make the right investments, executive teams should ask two sets of questions:

— Cybersecurity. How do we focus on the right topics and spend the right amount of money? How do we measure effectiveness (or, how much do our cyberefforts reduce our actual cyberrisks)? How do we know that we have the right team setup and can meet the cybersecurity challenge?

— IT infrastructure. What is our future IT-infrastructure strategy, and what are its implications for the business areas? Which benefits can the business expect from modernization? Are we set up to meet these expectations? What is our long-term plan for the areas not covered by modernization activities?

Leading airlines have started to address these challenges by setting up combined IT-infrastructure-modernization and cybersecurity programs with joint governance, harnessing synergies from both, and building alignment from the beginning. This helps to create transparency on the initial IT baseline, for example, to optimize overlaps for scarce resources, such as in architecture, and drive the negotiation (or renegotiation) of supplier contracts. Finding the right talent to strengthen the organization and drive these activities can make a decisive difference in the success of a transformation. For a case study of how one company approached the challenge, see sidebar, "How a leading airline modernized its IT infrastructure and increased its cyberresilience."

The time to act is now

More than four billion airline passengers will take cybersecurity for granted when they book flights this year. Additionally, they will expect to reach their destinations with few delays and with their luggage, resting assured that their payment and identity data are not for sale somewhere on the "darknet."

Complex, global IT systems that rely heavily on legacy components will remain vulnerable to breaches and failures. A range of attackers, including bad actors from outside the industry, will continue to look for ways in. The resiliency of airline business will depend on how well—and how quickly—the industry addresses shifting cyberrisks and modernizes IT applications and infrastructure in an

How a leading airline modernized its IT infrastructure and increased its cyberresilience

At the end of 2017, after having suffered from various IT-stability challenges and cyberincidents, a leading European airline decided to act: it started to develop an adjusted IT target picture. The goals of the target picture included increased operational stability, participation in technical innovation, and easier disaster recovery. The airline defined a holistic IT-infrastructure-transformation program to reduce the dependency on its single vendor, covering all IT infrastructure layers:

— IT management. Taking control of central components of the IT landscape and building strong provider-management capabilities put the airline in a position to integrate and steer multiple providers effectively.

— Network. Redesigning the global network allowed integration of new providers in a more flexible way and reduced the risk of single points of failure.

— Cloud and data center. Establishing a partnership with a strategic provider allowed the use of public-cloud benefits throughout the group.

— End-user computing. Increasing in-house capabilities enabled more self-control during important modernizations of parts of the environment, reducing the dependency on the primary outsourcing partner.

In parallel, the airline initiated a holistic cybersecurity program, systematically targeting blind spots across its operating model and value chain, following a risk-based approach. The program executed a multiyear road map to anchor cybersecurity as a core function within the organization, going far beyond classical IT. The initial phase involved creating transparency in generating a baseline on the current situation and risks. Then the airline developed a cybersecurity strategy that covered all business domains, established governance at the group level to decide on and control the implementation of risk-reducing initiatives, and began to execute.

As a result, the airline's IT organization professionalized its multiprovider management, regained control over its IT by introducing competition, and paved the way to leverage innovation from public cloud service providers at scale. In addition, it improved its overall IT stability and cyberresilience by systematically addressing high-risk blind spots, implementing a cyber fusion center, and anchoring cybersecurity considerations in all parts of its operating model.

increasingly digital world.

New hardware and software, innovative suppliers, and top talent can all help airlines harness the benefits of digitization and minimize the risks. But as the landscape continues to shift, IT needs to change structurally. Airlines need to anchor cybersecurity as a protector and IT infrastructure as an enabler of innovation on top of the chief information officer's agenda. Otherwise, powerful new technologies will not be harnessed to deliver maximum value, acquisition of IT talent will become more difficult, reliance on current legacy suppliers will increase, and ultimately, business opportunities, balance sheets, and corporate and personal reputations will be put at severe risk.

Thomas Elsner is a partner in McKinsey's Munich office, where **Christoph Fuchs** is an associate partner; **Benjamin Klein** is a consultant in the Berlin office, where **Wolf Richter** is a partner.

Designed by Global Editorial Services