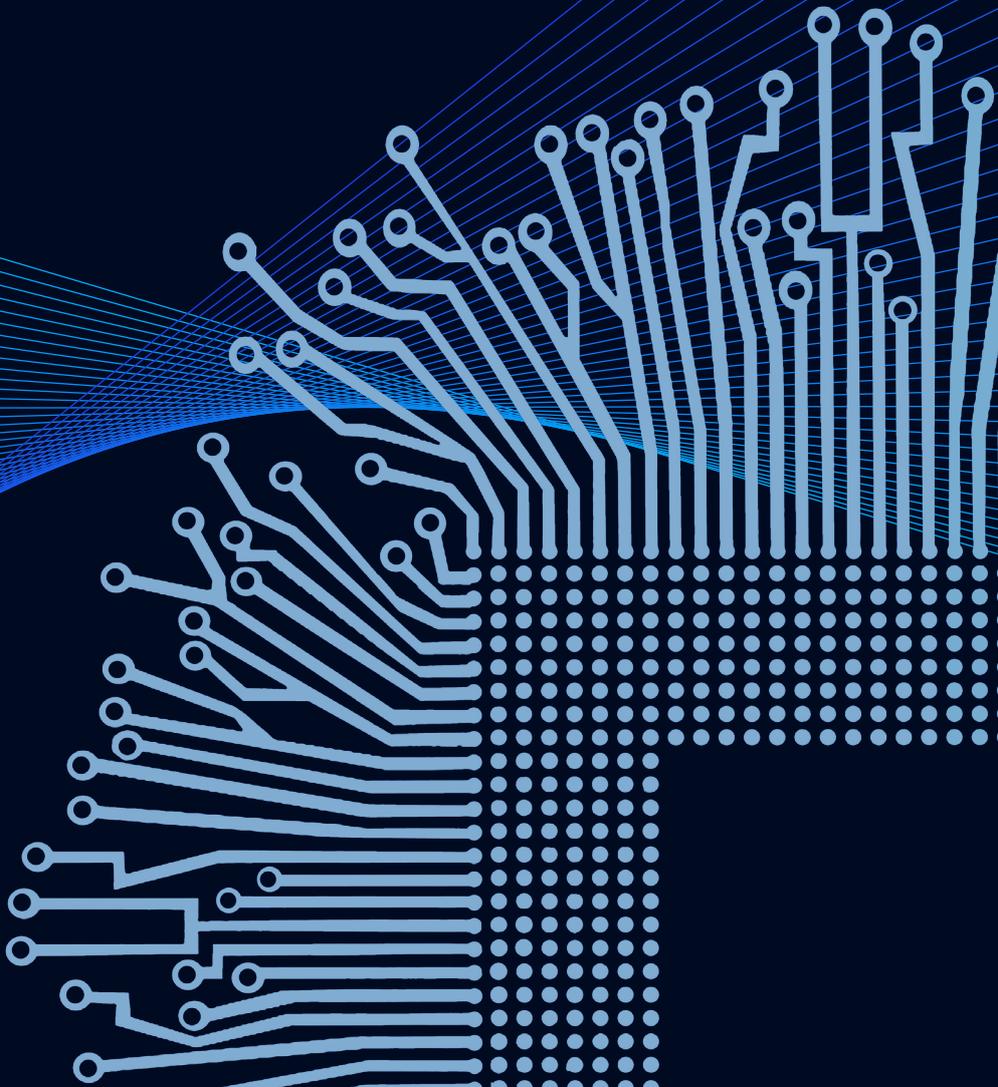


Safeguarding against cyberattack in an increasingly digital world

As part of its strategic partnership with Viva Technology, **McKinsey & Company** is publishing a series of articles looking at seven areas of technology that are potentially the most disruptive: Quantum computing, Cybersecurity, Connectivity & 5G, Cloud computing, AI, Digital ID, and Biotechnologies; as well as two major shifts for society: Future of work and Digital ecosystems.



Safeguarding against cyberattack in an increasingly digital world

The threat of cyberattack is universal. Factors such as digitization, greater use of online services and a rapid rise in working from home have all increased cyber risk. But there are things businesses can do to safeguard their organizations.

By Jim Boehm, James Kaplan, and Wolf Richter

All industries face the threat of cyberattack. According to a prior McKinsey survey, 75 percent of experts, across many industries, consider cyberrisk to be a top concern.¹

Until recently, financial firms were the primary targets. Risks for banks arise from diverse factors including vulnerabilities to fraud and financial crime inherent in automation and digitization; massive growth in transaction volumes; and greater integration of financial systems within countries and internationally.

Today, due to digitization and automation, the threat is universal. Added to this, the recent COVID-19 pandemic has intensified the danger of cyberattack, across all industries. Changes in working conditions have made it harder for companies to maintain security. Large-scale adoption of work-from-home technologies, heightened activity on customer-facing networks, and greater use of online services all present fresh openings, which cyber attackers have been quick to exploit.

The overarching challenge for chief information security officers (CISOs) and cybersecurity teams will be protecting their institutions against cyberthreats while maintaining business continuity.

¹ Six ways CEOs can promote cybersecurity in the IoT age, McKinsey & Company, August 2017, McKinsey.com.

Digitization increases the risk of cyberattack, and this is exacerbated by the COVID-19 pandemic

All industries face greater exposure to cyberthreats due to increasing digitization. For example, in the airline industry, digital innovation across the value chain—combined with the sheer volume of customer data airlines possess—has made them a hot target for cybercriminals. Various cyberincidents have demonstrated the need for airlines to upgrade IT and operational technology systems to reduce risk and build resiliency into their heavily digitized operating models. In 2019, the United Kingdom imposed a \$230 million fine on a European airline for a breach caused by security vulnerabilities in its website. And in 2018, hackers penetrated unpatched servers and access controls of an Asian airline to steal the personal data of 9.4 million customers.²

Additionally, 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.

Exhibit 1 shows a snapshot of recent, publicly reported IT and cyberincidents in the airline industry.

75%

of experts, across many industries, consider cyber risk to be a top concern³

² *How airlines should manage IT failures and security breaches to improve operational stability*, McKinsey & Company, November 2019, McKinsey.com.

³ *Six ways CEOs can promote cybersecurity in the IoT age*, McKinsey & Company, August 2017.

The airline industry has had several recent system 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 cyber-intrusion on its commercial-aircraft business-information system, resulting in unauthorized access to data and compromised professional-contact and IT-identification details of some employees

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 data (including name, date of birth, passport number, and historical travel information) compromised sensitive user information of up to **9.4 million passengers**

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

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 hrs**; 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

● April 2019:

Airline (AMERICA)

Global computer system outage grounded flights for several hours, causing large scale cancellations across several airlines

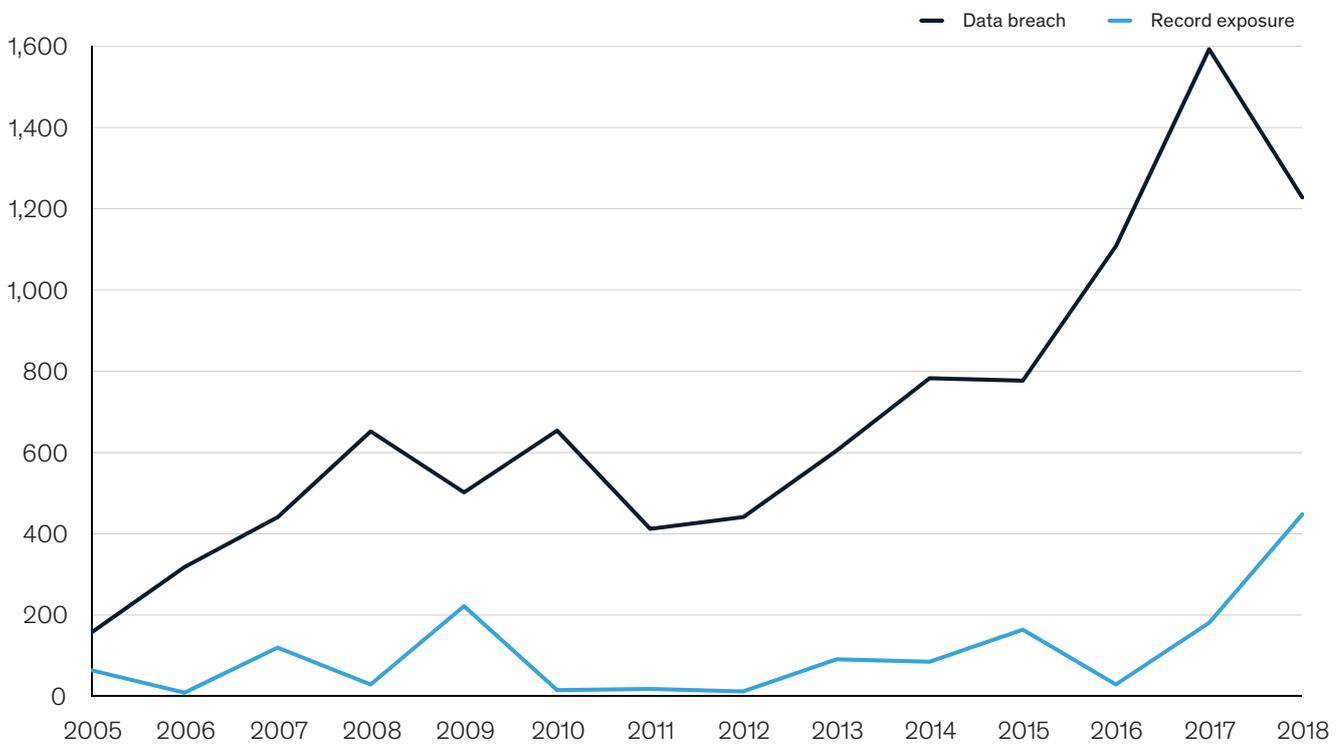
According to Identity Theft Resource Center statistics for the United States, despite a recent decline in the total number of data breaches to about 1.2 billion, the number of records exposed has grown by about 15 percent a year since 2005 to more than 447 million in 2018 (Exhibit 2).⁴

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.

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; McKinsey analysis, How airlines should manage IT failures and security breaches to improve operational stability, McKinsey & Company, November 2019

⁴ How airlines should manage IT failures and security breaches to improve operational stability, McKinsey & Company, November 2019, McKinsey.com.

The response to COVID-19 has increased cyber risk

Physical distancing means many workers are staying home and making greater use of videoconferencing services, collaboration platforms, and other digital tools to do business. In their free time, they are also going online more frequently to shop, read, chat, play, and stream. All these behaviors put immense stress on cybersecurity controls and operations. Several major vulnerabilities stand out:

First, a broad shift toward work-from-home arrangements has amplified long-standing cybersecurity challenges and opened multiple vectors for cyberattacks (Exhibit 3). Second, social-engineering ploys—to gain information, money, or access to protected systems—are on the rise, such

as attackers posing as help-desk teams, health workers or investors in virus-related response activities. Finally, cyber attackers are using websites with weak security to deliver malware, in some instances using domains and websites created to spread information and resources to combat COVID-19.

As the COVID-19 outbreak progresses and alters the functioning of our socioeconomic systems, cyber attackers will continue their efforts to exploit our fears and our digital vulnerabilities. To remain vigilant and effective, CISOs will need new tactics, particularly in two areas: securing work-from-home arrangements at scale; and supporting high levels of consumer-facing network traffic.

Exhibit 3

Shifting to work-from-home arrangements can open multiple vectors for cyberattacks.



Changes in app-access rights

Under existing policies, access to apps differs based on criticality and cyberrisk appetite (e.g., data infiltration, data-protection loss), from less critical apps accessible from almost anywhere (e.g., public network) to apps accessible through extranet, apps accessible only through VPN, and, ultimately, critical apps accessible only on site (e.g., trading, treasury)

Remote working can require organizations to widen access rights by enabling off-site access to some of the most critical apps, which can increase cyberrisk

Some users might not have strong multifactor authentication, because their access rights are usually limited; change in access rights, combined with weak authentication, constitutes a further threat



Use of personal devices and tools

Some employees may have been enabled to work from their own personal devices, but because these devices are not centrally controlled (for patching, network-access control, and endpoint data-protection systems), they can introduce cybersecurity vulnerabilities

To get work done, many employees use consumer-grade tools, accounts, and devices and share data over nonsecure and noncontrolled channels



Lack of social control

Click-through rates for phishing emails and success rates of fake call-center agents can increase if employees no longer maintain a "human protection shield" by asking coworkers about suspicious emails or calls

Source: McKinsey analysis – *Cybersecurity's dual mission during the coronavirus crisis*, McKinsey & Company, March 2020

How leaders can manage cyber risk

Given the gravity, complexity, and growing number of risks that businesses face, executives need ways to set priorities and sequence their cybersecurity and digitization investments. Based on our experience in serving 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. Managing cyber risk requires focus in four main areas: **assessing vulnerabilities with a quantitative risk analysis; reviewing cloud architecture and security capabilities; muscling up incident response and recovery capabilities;** and prioritizing a cybersecurity **budget**, including building a skilled **talent** pool and optimizing resources through **automation**.

Assess your vulnerabilities performing 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, companies 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 company at risk but are not yet covered by existing cyberactivities.

We recommend that cybersecurity leaders assess their organization's current vulnerability through a quantitative risk analysis including patch management practices; and build metrics and a dashboard to report regularly on the identified vulnerabilities and patch releases to CISO.

Review cloud architecture and security capabilities

A company should build an IT architecture and operating model that best supports its growth, digitization, and business model. In reviewing cloud architecture, it is important to first understand what data you are putting in the cloud now and to minimize the presence of sensitive information there. CISOs should also implement a holistic cloud security strategy—emphasizing access management, threat monitoring and incident response. Additionally, it is advisable to conduct regular penetration and vulnerability testing and audit reviews to ensure your cloud environment is secure.

Muscle up incident response and recovery capabilities

The tragic Covid-19 pandemic has shown that it is critical for companies to have robust incident response and recovery capabilities. All companies should have systems in place for monitoring and develop a response plan for supply chain cyberdisruptions. It is also advisable to continuously assess and refresh the incident response and recovery program based on your particular business risks and emerging threats, for example by hosting regular table-top exercises on emerging threats, and conducting comprehensive resilience exercises to test response and recovery capacities.

In the context of the pandemic, new tactics can help cybersecurity leaders to safeguard their organizations. The COVID-19 response has presented CISOs and their teams with two immediate priorities: One is securing work-from-home arrangements on an unprecedented scale; the other is maintaining the confidentiality, integrity, and availability of consumer-facing network traffic as volumes spike—partly as a result of the additional time people are spending at home. Recent discussions with cybersecurity leaders suggest that certain actions are particularly helpful in fulfilling these two priorities, in three areas: technology, people and processes.

Technology:

Work from home arrangements. Make sure required controls are in place—for example, accelerate patching for critical systems, scale up multifactor authentication and install controls for facility-based applications that have been migrated to remote access.

Consumer-facing network traffic. Ensure sufficient capacity by putting in place technical building blocks such as a web-application firewall, secure-sockets-layer (SSL) certification, network monitoring, anti-distributed denial of service, and fraud analytics.

People: Even with stronger technology controls, employees working from home must still exercise good judgment to maintain security. To help employees understand the risks, businesses need to communicate effectively and creatively. Focus on what to do—rather than what not to do—and increase awareness of social engineering ploys. Also identify and monitor high-risk users such as those working with confidential data.

Processes:

Work from home arrangements. Few business processes are designed to support extensive work from home, so most lack the right embedded controls. Promote resilience by supporting secure remote-working tools, testing and adjusting IR and BC/DR capabilities and securing physical documents. Also, take steps to expand monitoring and clarify incident-response protocols.

Consumer-facing network traffic. Customers, employees, and vendors all play some part in maintaining the confidentiality, integrity, and availability of web-facing networks. Integrate and standardize security activities, by, for example, integrating fraud prevention capabilities with the SOC, offer guidelines to help consumers solve some problems themselves, particularly during periods of peak use.

Prioritize cybersecurity budget, build a skilled talent pool & optimize resources through automation

Post pandemic, it will be even more critical for organizations to find ways to cover the rising costs of IT to meet innovation and cybersecurity requirements. 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.

To keep their organization on track and make the right investments, cybersecurity executives should ask and answer the following questions regarding budget, talent and automation:

Budget:

- How do we focus on the right topics and spend the right amount of money?

By evaluating cyber spending against key risks and its impact on them, making sure this is proportional.

- How do we measure effectiveness and evaluate how much our cyberefforts reduce our actual cyber risks?

By assessing ROI for cyber investments based on risk reduction.

Talent:

- How do we know we have the right team to meet the cybersecurity challenge?

By reviewing your cyber and risk teams' RACI, the complexity of your solutions and identifying skillset gaps. Also, by providing continuous learning opportunities to help employees adapt to new tools and technologies.

Automation:

- What is our future IT-infrastructure strategy, and what are its implications for the business areas?

- What benefits can the business expect from modernization, and are we set up to meet these expectations?

To answer these questions, identify operational processes that can be transformed through automation to reduce human overhead.

All businesses, across all industries, face the risk of cyberattack. The COVID-19 pandemic may have exacerbated this risk as changes in working conditions have made it harder for companies to maintain security. But there are steps businesses can take to manage security breaches, increase cyberresilience and improve operational stability. Tactics to help businesses safeguard their organizations while ensuring business continuity center on two priorities: securing work-from-home arrangements at scale; and supporting high levels of consumer-facing network traffic.

Jim Boehm is a McKinsey partner in Washington DC, **James Kaplan** is a McKinsey partner in New York, and **Wolf Richter** is a McKinsey partner in Berlin.

The authors wish to thank the authors of the following publications, upon which this work is based: [Cybersecurity's dual mission during the coronavirus crisis](#), McKinsey & Company, March 2020; [Cybersecurity tactics for the coronavirus pandemic](#), McKinsey & Company, March 2020; [How airlines should manage IT failures and security breaches to improve operational stability](#), McKinsey & Company, November 2019; [The cybersecurity posture of financial-services companies: IIF/ McKinsey Cyber Resilience Survey](#), McKinsey & Company, April 2020; [Financial crime and fraud in the age of cybersecurity](#), McKinsey & Company, October 2019.

The authors also wish to thank Amine Aït-Si-Selmi, Marion Castel, and Mathilde Castet for their contributions to this article.

June 2020
Copyright © McKinsey & Company

www.mckinsey.com

 @McKinseyFrance

 McKinseyFrance

