McKinsey & Company

McKinsey Explainers

What is cybersecurity?

It’s what organizations do to protect their own and their customers’ data from malicious attacks.

April 2023

Hot data. The internet isn't always a safe space. Cyberattacks are on the rise, and there's no indication that they will stop anytime soon.

As a result of this uptick, everyone is on red alert: consumers are paying more attention to where their data goes; governments are putting regulations in place to protect their populations; and organizations are spending more time, energy, and money to guard their operations against cybercrime.

For organizations, the increasing awareness of cyber risk, by consumers and regulators alike, doesn't have to spell trouble. In fact, the current climate could present savvy leaders with a significant growth opportunity. McKinsey research indicates that the organizations best positioned to build digital trust are more likely than others to see annual growth of at least 10 percent.

What's the current state of cybersecurity for consumers, regulators, and organizations? And how can organizations turn the risks into rewards? Read on to learn from McKinsey Insights.

What is a cyberattack?

Before we learn how organizations and individuals can protect themselves, let's start with what they're protecting themselves against. What is a cyberattack? Simply, it's any malicious attack on a computer system, network, or device to gain access and information. There are many different types of cyberattacks. Here are some of the most common ones:

— *Malware* is malicious software, including spyware, ransomware, and viruses. It accesses a network through a weakness—for example, when a member of the network clicks on a fraudulent link or email attachment. Once malware controls a system, it can demand payment in exchange for access to that system (ransomware), covertly transmit information from the network (spyware), or install additional harmful software on the network. In 2021, ransomware attacks alone surged by 105 percent.

— *Phishing* involves a bad actor sending a fraudulent message that appears to come from a legitimate source, like a bank or a company, or from somebody with the wrong number. Phishing attacks are made through email, text, or social networks. Typically, the goal is to steal information by installing malware or by cajoling the victim into divulging personal details.

— *Man-in-the-middle attacks* are incidents in which an attacker comes between two members of a transaction to eavesdrop on personal information. These attacks are particularly common on public Wi-Fi networks, which can be easily hacked.

— *Denial-of-service attacks* flood systems with traffic to clog up bandwidth so that they can't fulfill legitimate requests. The goal of this type of attack is to shut down systems.

— *Password attacks* are mounted by cybercriminals who try to steal passwords by guesswork or trickery.

Individuals and companies can protect themselves against cyberattacks in a variety of ways—from passwords to physical locks on hard drives. Network security protects a wired or wireless computer network from intruders. Information security—such as the data protection measures in Europe's General Data Protection Regulation (GDPR)—protects sensitive data from unauthorized access. There are many more kinds of cybersecurity, including antivirus software and firewalls. Cybersecurity is big business: one tech research and advisory company estimates that businesses will spend more than $188 billion on information security in 2023.

Despite the extensive measures organizations implement to protect themselves, they often don't go far enough. Cybercriminals are constantly evolving their methods to take advantage of consumer shifts and newly exposed loopholes. When the world hastily shifted to remote work at the beginning of the pandemic, for example, cybercriminals took advantage of new software vulnerabilities to wreak havoc on computer systems. The Internet Crime Complaint Center of the US Federal Bureau of Investigation (FBI) reported a nearly 50 percent increase in suspected internet crime in 2020 from 2019. Reported losses exceeded $4.2 billion.

Which cybersecurity trends are projected over the next three to five years?

Cyber risk isn't static, and it never goes away. Only by taking a dynamic, forward-looking stance can companies keep up with the state of play and mitigate disruptions in the future. These three major cybersecurity trends may have the biggest implications for organizations:

1. *On-demand access to ubiquitous data and information platforms is growing.* Recent shifts toward mobile platforms and remote work require high-speed access to ubiquitous, large data sets. This dependency exacerbates the likelihood of a breach. Organizations collect more data than ever about their customers, so such a breach could be especially costly. To store, manage, and protect the data, organizations need new technology platforms.

2. *Hackers use AI, machine learning, and other technologies to launch increasingly sophisticated attacks.* Gone are the days of the hacker in a hoodie working alone in a room with blackout shades. Today, hacking is a multibillion-dollar industry, complete with institutional hierarchies and R&D budgets. Attackers using advanced tools such as AI, automation, and machine learning will cut the end-to-end life cycle of an attack from weeks to days or even hours. Other technologies and capabilities are making known forms of attacks, such as ransomware and phishing, easier to mount and more common.

3. *The growing regulatory landscape and continued gaps in resources, knowledge, and talent mean that organizations must continually evolve and adapt their cybersecurity approach.* Many organizations don't have enough knowledge, talent, and expertise on cybersecurity. The shortfall is growing as regulators increase their monitoring of cybersecurity in corporations.

These are the three cybersecurity trends McKinsey predicts for the next few years. Later in this *Explainer*, you'll learn how organizations can stay ahead of the curve.

How are regulators approaching cybersecurity?

As high-profile cyberattacks catapult data security into the international spotlight, policy makers are paying increased attention to how organizations manage the public's data. In the United States, the federal government and at least 45 states and Puerto Rico have introduced or considered more than 250 bills or resolutions that deal with cybersecurity. In Europe, the General Data Protection Regulation levies fines of up to 4 percent of global turnover against companies that fail to protect their customers' data.

How can US organizations prepare for new cyber regulations?

Some of the most significant compromises of essential services or information in recent years have involved attacks against large US companies. In 2021, the FBI received the highest number of cybercrime complaints and reported total losses in history: nearly 850,000 complaints, reflecting more than $6.9 billion in losses. New legislation will influence how companies report and disclose cybercrime and how they govern their efforts to fight it.

There are three steps US organizations can take to help prepare for new regulations.

— *Readiness.* Companies can increase their readiness for cyberattacks by double-checking their ability to detect and identify them and creating clear reporting processes. Existing

Companies can increase their readiness for cyberattacks by double-checking their ability to detect and identify them and creating clear reporting processes.

processes should be tested and refined through simulation exercises.

- *Response.* Companies can upgrade their response to cyberattacks by improving their ability to identify, contain, eradicate, and recover from them. They can, for example, establish crisis nerve centers, hire outside experts to cross-check their plans, and implement protocols to use alternative support and services during an attack.
- *Remediation.* In the aftermath of a crisis, companies can reflect on lessons learned and apply them to better strategies for greater resilience.

How can cybersecurity technology and service providers help?

Cyberattacks are on track to cause $10.5 trillion a year in damage by 2025. That's a 300 percent increase from 2015 levels. To protect against the onslaught, organizations around the world spent around $150 billion on cybersecurity in 2021, and this sum is growing by 12.4 percent a year. But even that is probably not enough: threat volumes are predicted to rise in coming years.

The gap between the current market and the total addressable market is huge; only 10 percent of the security solutions market has currently been penetrated. The total opportunity is a staggering $1.5 trillion to $2 trillion.

Given current trends, cybersecurity providers can focus on four key areas:

Cloud technologies. For the foreseeable future, migration to the cloud will continue to dominate the technology strategies of many organizations. Providers should therefore be able to protect both general and specialized cloud configurations.

Pricing mechanisms. Most cyber solutions currently on the market are not aimed at small- to medium-sized businesses. Cybersecurity providers can capture this market by creating products tailored to it.

Artificial intelligence. There's huge potential for innovative AI and machine learning in the cybersecurity space. But operators struggle to trust autonomous intelligent cyberdefense platforms and products. Providers should instead develop AI and machine-learning products that make human analysts more efficient.

Managed services. Demand for full-service offerings is set to rise by as much as 10 percent annually over the next three years. Providers should develop bundled offerings that include hot-button use cases. And they should focus on outcomes, not technology.

What is ransomware? What kind of damage can it do?

Malware that manipulates a victim's data and holds it for ransom by encrypting it is ransomware. In recent years, it has achieved a new level of sophistication, and demands for payment have rocketed into the tens of millions of dollars. The "smash and grab" operations of the past have morphed into a long game: hackers lurk undetected within their victims' environments to find the most valuable information and data. And the situation is predicted only to worsen: the market research organization and *Cybercrime Magazine* publisher Cybersecurity Ventures estimates that the cost of ransomware could reach $265 billion by 2031. Here are some specific costs that companies have faced as a result of ransomware attacks:

— Colonial Pipeline paid a $4.4 million ransom after the company shut down operations.

— Global meat producer JBS paid $11 million.

— Global insurance provider CNA Financial paid a reported $40 million.

— A ransomware attack on US software provider Kaseya targeted its remote computer management tool and endangered up to 2,000 companies around the world.

These figures don't include costs such as payments to third parties—for instance, law, public-relations, and negotiation firms. Nor do they include the opportunity costs of having executives and specialized teams turn away from their day-to-day roles for weeks or months to deal with an attack or with the resulting lost revenues.

What can organizations do to mitigate future cyberthreats?

Cybersecurity managers ought to consider the following capabilities, which should be adjusted to the unique contexts of individual companies.

— *Zero-trust architecture (ZTA).* In this security system design, all entities—inside and outside the organization's computer network—are not trusted by default and must prove their trustworthiness. ZTA shifts the focus of cyberdefense away from the static perimeters around physical networks and toward users, assets, and resources, thus mitigating the risk from decentralized data.

— *Behavioral analytics.* These tools can monitor employee access requests or the health of devices and identify anomalous user behavior or device activity.

— *Elastic log monitoring for large data sets.* Thanks to advances in big data and the Internet of Things (IoT), data sets are larger than ever. The sheer volume of data that must be monitored makes keeping track of who's accessing it all the more challenging. Elastic log monitoring allows companies to pull log data from anywhere in the organization into a single location and then to search, analyze, and visualize it in real time.

— *Homomorphic encryption.* This method allows users to work with encrypted data without first decrypting it, thus giving third parties and other collaborators safe access to large data sets.

— *Risk-based automation.* As digitization levels increase, organizations can use automation to handle lower-risk and rote processes, freeing up other resources for higher-value activities.

— *Defensive AI and machine learning for cybersecurity.* Since cyberattackers are adopting AI and machine learning, cybersecurity teams must scale up the same technologies. Organizations can use them to detect and fix noncompliant security systems.

— *Technical and organizational responses to ransomware.* As the sophistication, frequency, and range of ransomware increase, organizations must keep up with it.

— *Secure software development.* Companies should embed cybersecurity in the design of software from inception. Security and technology risk teams should engage with developers throughout each stage of development. Security teams should also adopt more systematic approaches to problems, including agile and kanban.

- *Infrastructure and security as code.* Standardizing and codifying infrastructure and control-engineering processes can simplify the management of complex environments and increase a system's resilience.

- *Software bill of materials.* As compliance requirements grow, organizations can mitigate the administrative burden by formally detailing all components and supply chain relationships used in software. This approach also helps ensure that security teams are prepared for regulatory inquiries.

How can a 'security champions' program promote a stronger internal cybersecurity culture?

An organization is only as good as its people, and its security is only as strong as their understanding of why security matters. McKinsey spoke with MongoDB, a data platform development company, about how it established a security champions program to help its employees make security a top priority.

To raise awareness of security issues and create a robust security culture, MongoDB rebooted its security champions program during the pandemic. As of October 2022, the program had hosted more than 20 events, bringing employees together to learn about security through scenario planning and to participate in team-building activities, like capture the flag.

MongoDB's goal is to have 10 percent of its employees participate in the security champions program. Participants vow to give it a few hours each week and then serve as security ambassadors to their teams and departments. The company's leaders also see the program as a vehicle for training because it helps upskill employees, who can then take positions on the security and compliance teams. "This is great," says MongoDB chief information security officer Lena Smart, "during a time when it is quite difficult to find skilled [cybersecurity] talent."

How does the company know that the program is working? "We look at trends over time," says Felix Chen, cybersecurity education and advocacy senior

Standardizing and codifying infrastructure and control-engineering processes simplify the management of complex environments and increase a system's resilience.

analyst at MongoDB. "For example, in our phishing-simulation campaigns, we look at how many people clicked on a phishing link. We look at event attendance and reported vulnerabilities. And, importantly, we communicate our progress with leadership."

How can cybersecurity talent help mitigate cyber risk?

Technical controls and capabilities are, and will always be, necessary to secure the environment of any organization. But it will be even better positioned to reduce its exposure to cybersecurity risk if it adopts a new approach to hiring cybersecurity talent. That approach focuses on preplanning and understanding cybersecurity needs holistically. Hiring cybersecurity workers isn't easy, especially given the global shortage of skilled ones: according to a 2022 study, there's a cybersecurity workforce gap of 3.4 million.

One way to tackle the problem is the *talent-to-value protection approach*. Using this approach, leaders define the roles that stand to reduce the most risk or create the most security value. Roles identified as priorities should be filled as soon as possible. This approach allows organizations to hire the right people at the right times, ensuring that spending on personnel is aligned with growth aspirations.

Here are three steps to implementing talent-to-value protection:

1. *Identify* the most important cybersecurity activities given the organization's needs, as well as the most pressing risks that should be mitigated. These can be determined through risk modeling and ranking potential vulnerabilities by the degree of risk they pose.

2. *Define* the priority roles that reduce risk most effectively.

3. *Build* job descriptions for these priority roles and determine whether upskilling or hiring is the best way to fill each of them.

For a more in-depth exploration of these topics, see McKinsey Digital's Cybersecurity *collection. Learn more about McKinsey's Risk & Resilience Practice—and check out cybersecurity-related job opportunities if you're interested in working at McKinsey.*

Articles referenced include:

— "New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers," October 27, 2022, Bharath Aiyer, Jeffrey Caso, Peter Russell, and Marc Sorel

— "Building a cybersecurity culture from within: An interview with MongoDB," October 10, 2022, Amy Berman, Felix Chen, James Kaplan, Charlie Lewis, and Lena Smart

— "Software bill of materials: Managing software cybersecurity risks," September 19, 2022, Tucker Bailey, Justin Greis, Matt Watters, and Josh Welle

— "Why digital trust truly matters," September 12, 2022, Jim Boehm, Liz Grennan, Alex Singla, and Kate Smaje

— "Creating a technology risk and cyber risk appetite framework," August 25, 2022, James Kaplan, Charlie Lewis, Lucy Shenton, Daniel Wallance, and Zoe Zwiebelmann

— "Perspectives on model risk management of cybersecurity solutions in banking," August 22, 2022, Juan Aristi Baquero, Rich Isenberg, Chirag Jain, Pankaj Kumar, Christophe Rougeaux, and Marc Taymans

— "Localization of data privacy regulations creates competitive opportunities," June 30, 2022, Satyajit Parekh, Stephen Reddin, Kayvaun Rowshankish, Henning Soller, and Malin Strandell-Jansson

Find more content like this on the
McKinsey Insights App

Scan • Download • Personalize

- “Securing your organization by recruiting, hiring, and retaining cybersecurity talent to reduce cyberrisk,” June 29, 2022, Venky Anant, Michael Glynn, Justin Greis, Nick Kosturos, Ida Kristensen, Charlie Lewis, and Leandro Santos

- “Cybersecurity legislation: Preparing for increased reporting and transparency,” June 17, 2022, Tucker Bailey, Justin Greis, Matt Watters, and Josh Welle

- “Cybersecurity trends: Looking over the horizon,” March 10, 2022, Jim Boehm, Dennis Dias, Charlie Lewis, Kathleen Li, and Daniel Wallance

- “Ransomware prevention: How organizations can fight back,” February 14, 2022, Jim Boehm, Franz Hall, Rich Isenberg, and Marissa Michel

- “The unsolved opportunities for cybersecurity providers,” January 5, 2022, Bharath Aiyer, Jeffrey Caso, and Marc Sorel

Designed by McKinsey Global Publishing
Copyright © 2023 McKinsey & Company. All rights reserved.