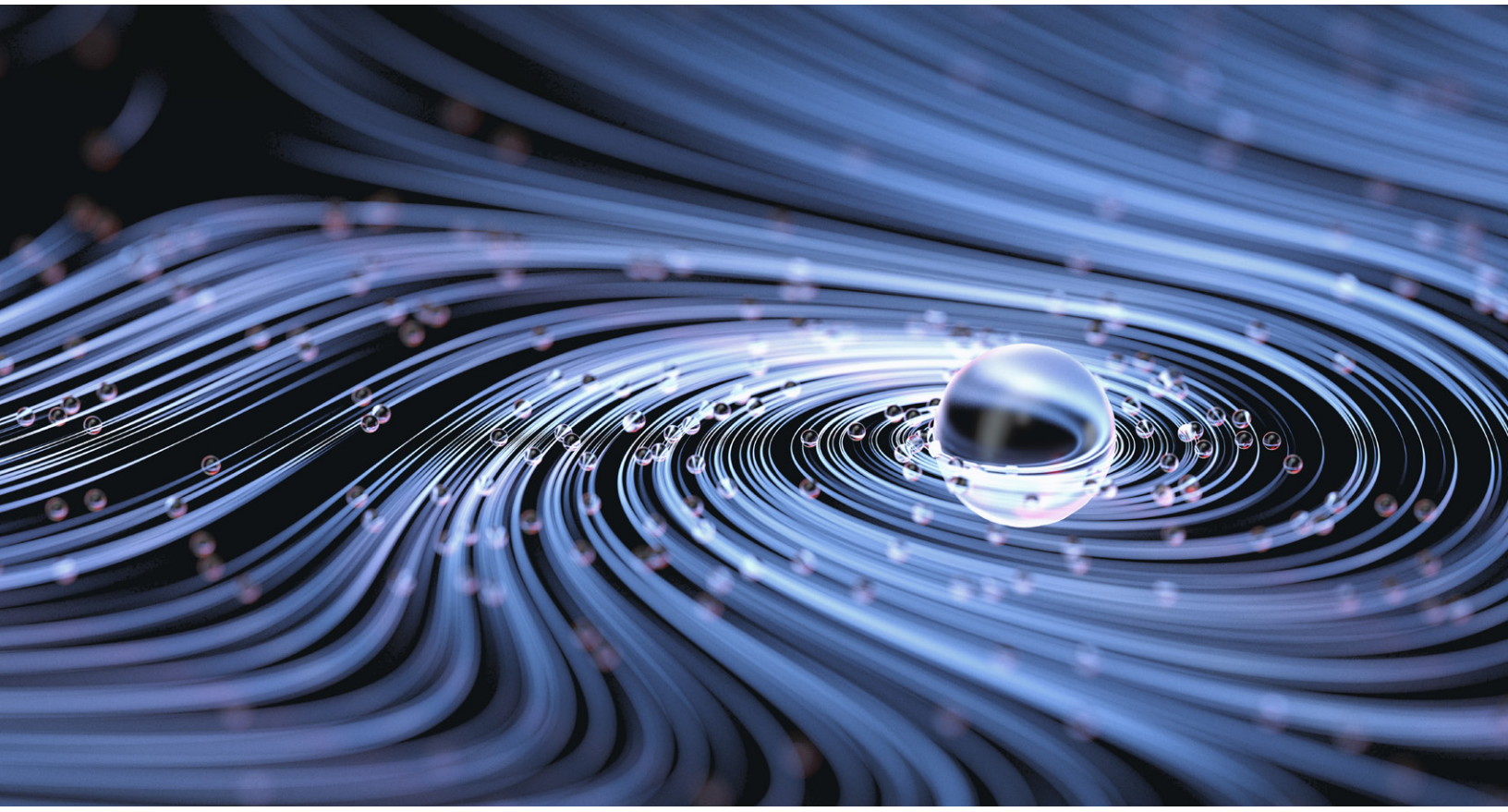
McKinsey & Company

Risk & Resilience Practice

Cybersecurity trends: Looking over the horizon

McKinsey examines three of the latest cybersecurity trends and their implications for organizations facing new and emerging cyberrisks and threats.

This article is a collaborative effort by Jim Boehm, Dennis Dias, Charlie Lewis, Kathleen Li, and Daniel Wallance, representing views from McKinsey's Risk & Resilience Practice.



March 2022

Cybersecurity has always been a never-ending race, but the rate of change is accelerating. Companies are continuing to invest in technology to run their businesses. Now, they are layering more systems into their IT networks to support remote work, enhance the customer experience, and generate value, all of which creates potential new vulnerabilities.

At the same time, adversaries—no longer limited to individual actors—include highly sophisticated organizations that leverage integrated tools and capabilities with artificial intelligence and machine learning. The scope of the threat is growing, and no organization is immune. Small and midsize enterprises, municipalities, and state and federal governments face such risks along with large companies. Even today's most sophisticated cybercontrols, no matter how effective, will soon be obsolete.

In this environment, leadership must answer key questions: "Are we prepared for accelerated digitization in the next three to five years?" and, more specifically, "Are we looking far enough forward to understand how today's technology investments will have cybersecurity implications in the future?" (Exhibit 1).

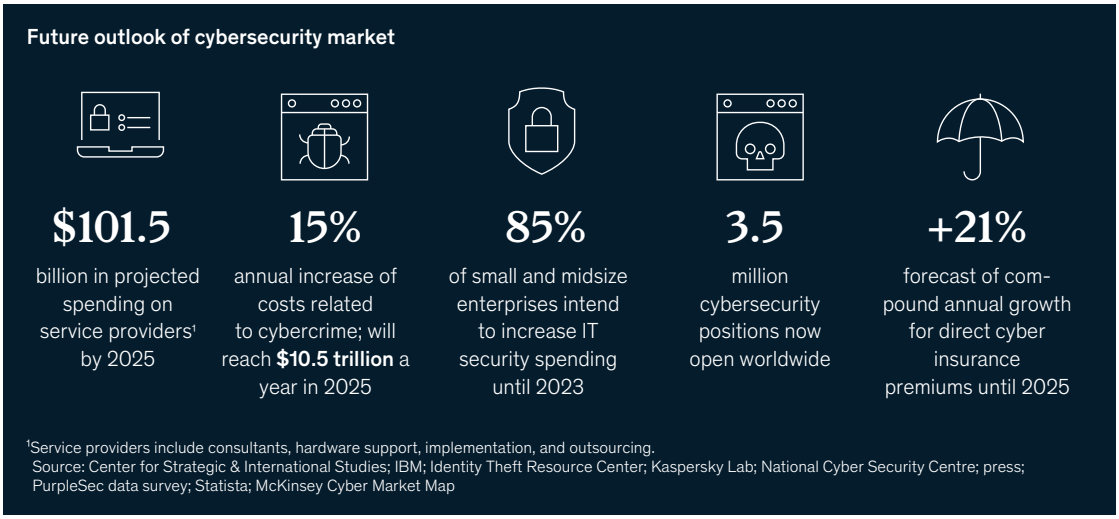
McKinsey's work helping global organizations reinforce their cyberdefenses shows that many companies recognize the need to achieve a step change in their capabilities for cybersecurity and to ensure the resilience of their technology. The solution is to reinforce their defenses by looking forward—anticipating the emerging cyberthreats of the future and understanding the slew of new defensive capabilities that companies can use today and others they can plan to use tomorrow (see sidebar, "Maintaining vigilance over time").

Three cybersecurity trends with large-scale implications

Companies can address and mitigate the disruptions of the future only by taking a more proactive, forward-looking stance—starting today. Over the next three to five years, we expect three major cybersecurity trends that cross-cut multiple technologies to have the biggest implications for organizations.

Exhibit 1

Cyberattacks are on the rise, and market indicators reflect a fear of further increases.



Maintaining vigilance over time

Proactively mitigating cybersecurity threats and evaluating over-the-horizon cybersecurity capabilities is not a one-time process. It requires ongoing vigilance and a structured approach to ensure that organizations proactively scan the environment and adjust their cyber stance accordingly. We see leading organizations adopting a three-step process:

1. Validate cybercontrols—especially emerging ones—technically to ensure your readiness for evolving threats and technologies.
2. Challenge your cyberstrategy to refresh the road map with emerging capabilities and approaches.
3. Adopt a formal program of record to continually review your cyberstrategy, technologies, and processes against shifts in cybersecurity trends.

1. On-demand access to ubiquitous data and information platforms is growing

Mobile platforms, remote work, and other shifts increasingly hinge on high-speed access to ubiquitous and large data sets, exacerbating the likelihood of a breach. The marketplace for web-hosting services is expected to generate $183.18 billion by 2026.[1] Organizations collect far more data about customers—everything from financial transactions to electricity consumption to social-media views—to understand and influence purchasing behavior and more effectively forecast demand. In 2020, on average, every person on Earth created 1.7 megabytes of data each second.[2] With the greater importance of the cloud, enterprises are increasingly responsible for storing, managing, and protecting these data[3] and for meeting the challenges of explosive data volumes. To execute such business models, companies need new technology platforms, including data lakes that can aggregate information, such as the channel assets of vendors and partners, across environments. Companies are not only gathering more data but also centralizing them, storing them on the cloud, and granting access to an array of people and organizations, including third parties such as suppliers.

Many recent high-profile attacks exploited this expanded data access. The Sunburst hack, in 2020, entailed malicious code spread to customers during regular software updates. Similarly, attackers in early 2020 used compromised employee credentials from a top hotel chain's third-party application to access more than five million guest records.[4]

2. Hackers are using AI, machine learning, and other technologies to launch increasingly sophisticated attacks

The stereotypical hacker working alone is no longer the main threat. Today, cyberhacking is a multibillion-dollar enterprise,[5] complete with institutional hierarchies and R&D budgets. Attackers use advanced tools, such as artificial intelligence, machine learning, and automation. Over the next several years, they will be able to expedite—from weeks to days or hours—the end-to-end attack life cycle, from reconnaissance

[1] Fortune Business Insight.
[2] "Data never sleeps 6.0," Domo.
[3] John Gantz, David Reinsel, and John Rydning, *The digitization of the world: From edge to core*, IDC, November 2018.
[4] David Uberti, "Marriott reveals breach that exposed data of up to 5.2 million customers," *Wall Street Journal*, March 31, 2020.
[5] "Cybersecurity: Hacking has become a $300 billion dollar industry," InsureTrust.

Cyberrisk management has not kept pace with the proliferation of digital and analytics transformations, and many companies are not sure how to identify and manage digital risks.

through exploitation. For example, Emotet, an advanced form of malware targeting banks, can change the nature of its attacks. In 2020, leveraging advanced AI and machine-learning techniques to increase its effectiveness, it used an automated process to send out contextualized phishing emails that hijacked other email threats—some linked to COVID-19 communications.

Other technologies and capabilities are making already known forms of attacks, such as ransomware and phishing, more prevalent. Ransomware as a service and cryptocurrencies have substantially reduced the cost of launching ransomware attacks, whose number has doubled each year since 2019. Other types of disruptions often trigger a spike in these attacks. During the initial wave of COVID-19, from February 2020 to March 2020, the number of ransomware attacks in the world as a whole spiked by 148 percent, for example.[6] Phishing attacks increased by 510 percent from January to February 2020.[7]

3. Ever-growing regulatory landscape and continued gaps in resources, knowledge, and talent will outpace cybersecurity

Many organizations lack sufficient cybersecurity talent, knowledge, and expertise—and the shortfall is growing. Broadly, cyberrisk management has not kept pace with the proliferation of digital and analytics transformations, and many companies are not sure how to identify and manage digital risks. Compounding the challenge, regulators are increasing their guidance of corporate cybersecurity capabilities—often with the same level of oversight and focus applied to credit and liquidity risks in financial services and to operational and physical-security risks in critical infrastructure.

At the same time, companies face stiffer compliance requirements—a result of growing privacy concerns and high-profile breaches. There are now approximately 100 cross-border data flow regulations. Cybersecurity teams are managing additional data and reporting requirements stemming from the White House Executive Order on Improving the Nation's Cybersecurity and the advent of mobile-phone operating systems that ask users how they want data from each individual application to be used.

Building over-the-horizon defensive capabilities

For each of these shifts, we see defensive capabilities that organizations can develop to mitigate the risk and impact of future cyberthreats. To be clear, these capabilities are not perfectly

[6] *VMware security blog*, "Amid COVID-19, global orgs see a 148% spike in ransomware attacks; finance industry heavily targeted," April 15, 2020.
[7] Brian Carlson, "Top cybersecurity statistics, trends, and facts," CSO, October 7, 2021.

mapped to individual shifts, and many apply to more than one. Management teams should consider all of these capabilities and focus on those most relevant to the unique situation and context of their companies (Exhibit 2).

Responses to trend one: Zero-trust capabilities and large data sets for security purposes
Mitigating the cybersecurity risks of on-demand access to ubiquitous data requires four cybersecurity capabilities: zero-trust capabilities, behavioral analytics, elastic log monitoring, and homomorphic encryption.

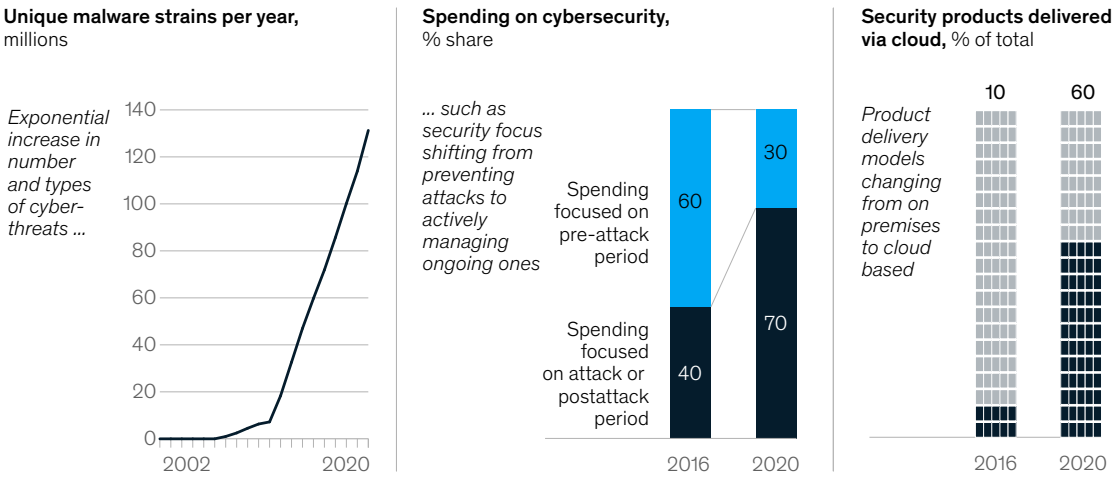
Zero-trust architecture (ZTA). Across industrial nations, approximately 25 percent of all workers now work remotely three to five days a week.[8] Hybrid and remote work, increased cloud access, and Internet of Things (IoT) integration create potential vulnerabilities. A ZTA shifts the focus of cyberdefense away from the static perimeters around physical networks and toward users, assets, and resources, thus mitigating the risk from decentralized data. Access is more granularly enforced by policies: even if users have access to the data environment, they may not have access to sensitive data. Organizations should tailor the adoption of zero-trust capabilities to the threat and risk landscape they actually face and to their business objectives. They should also consider standing up red-team testing to validate the effectiveness and coverage of their zero-trust capabilities.

Behavioral analytics. Employees are a key vulnerability for organizations. Analytics solutions can monitor attributes such as access requests or the health of devices and establish a baseline to identify anomalous intentional or unintentional user behavior or device activity. These tools can not only enable risk-based authentication and authorization but also orchestrate preventive and incident response measures.

Exhibit 2

As cyberthreats continue to increase in type and frequency, so too will cybersecurity spend.

Overall enterprise cybersecurity trends



Source: McKinsey anaylsis

[8] *Global surveys of consumer sentiment during the coronavirus crisis*, McKinsey.

Elastic log monitoring for large data sets. Massive data sets and decentralized logs resulting from advances such as big data and IoT complicate the challenge of monitoring activity. Elastic log monitoring is a solution based on several open-source platforms that, when combined, allow companies to pull log data from anywhere in the organization into a single location and then to search, analyze, and visualize the data in real time. Native log-sampling features in core tools can ease an organization's log management burden and clarify potential compromises.

Homomorphic encryption. This technology allows users to work with encrypted data without first decrypting and thus gives third parties and internal collaborators safer access to large data sets. It also helps companies meet more stringent data privacy requirements. Recent breakthroughs in computational capacity and performance now make homomorphic encryption practical for a wider range of applications.

Responses to trend two: Using automation to combat increasingly sophisticated cyberattacks

To counter more sophisticated attacks driven by AI and other advanced capabilities, organizations should take a risk-based approach to automation and automatic responses to attacks. Automation should focus on defensive capabilities like security operations center (SOC) countermeasures and labor-intensive activities, such as identity and access management (IAM) and reporting. AI and machine learning should be used to stay abreast of changing attack patterns. Finally, the development of both automated technical and automatic organizational responses to ransomware threats helps mitigate risk in the event of an attack.

Automation implemented through a risk-based approach. As the level of digitization accelerates, organizations can use automation to handle lower-risk and rote processes, freeing up resources for higher-value activities. Critically, automation decisions should be based on risk assessments and segmentation to ensure that additional vulnerabilities are not inadvertently created. For example, organizations can apply automated patching, configuration, and software upgrades to low-risk assets but use more direct oversight for higher-risk ones.

Use of defensive AI and machine learning for cybersecurity. Much as attackers adopt AI and machine-learning techniques, cybersecurity teams will need to evolve and scale up the same capabilities. Specifically, organizations can use these technologies and outlier patterns to detect and remediate noncompliant systems. Teams can also leverage machine learning to optimize workflows and technology stacks so that resources are used in the most effective way over time.

Technical and organizational responses to ransomware. As the sophistication, frequency, and range of ransomware attacks increase, organizations must respond with technical and operational changes. The technical changes include using resilient data repositories and infrastructure, automated responses to malicious encryption, and advanced multifactor authentication to limit the potential impact of an attack, as well as continually addressing cyber hygiene. The organizational changes include conducting tabletop exercises, developing detailed and multidimensional playbooks, and preparing for all options and contingencies—including executive response decisions—to make the business response automatic.

Responses to trend three: Embedding security in technology capabilities to address ever-growing regulatory scrutiny and resource gaps

Increased regulatory scrutiny and gaps in knowledge, talent, and expertise reinforce the need to build and embed security in technology capabilities as they are designed, built, and implemented. What's more, capabilities such as security as code and a software bill of materials help organizations to deploy security capabilities and stay ahead of the inquiries of regulators.

Secure software development. Rather than treating cybersecurity as an afterthought,

companies should embed it in the design of software from inception, including the use of a software bill of materials (described below). One important way to create a secure software development life cycle (SSDLC) is to have security and technology risk teams engage with developers throughout each stage of development. Another is to ensure that developers learn certain security capabilities best employed by development teams themselves (for instance, threat modeling, code and infrastructure scanning, and static and dynamic testing). Depending on the activity, some security teams can shift to agile product approaches, some can adopt a hybrid approach based on agile-kanban tickets, and some—especially highly specialized groups, such as penetration testers and security architects—can "flow to work" in alignment with agile sprints and ceremonies.

Taking advantage of X as a service. Migrating workloads and infrastructure to third-party cloud environments (such as platform as a service, infrastructure as a service, and hyperscale providers) can better secure organizational resources and simplify management for cyberteams. Cloud providers not only handle many routine security, patching, and maintenance activities but also offer automation capabilities and scalable services. Some organizations seek to consolidate vendors for the sake of simplicity, but it can also be important to diversify partners strategically to limit exposure to performance or availability issues.

Infrastructure and security as code. Standardizing and codifying infrastructure and control-engineering processes can simplify the management of hybrid and multicloud environments and increase the system's resilience. This approach enables processes such as orchestrated patching, as well as rapid provisioning and deprovisioning.

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. Like a detailed bill of materials, this documentation would list open-source and third-party components in a codebase through new software development processes, code-scanning tools, industry standards, and supply chain requirements. In addition to mitigating supply chain risks, detailed software documentation helps ensure that security teams are prepared for regulatory inquiries.

Digital disruption is inevitable and will lead to rapid technology-driven change. As organizations make large-scale investments in technology—whether in the spirit of innovation or from necessity—they must be aware of the associated cyberrisks. Attackers are exploiting the vulnerabilities that new technologies introduce, and even the best cybercontrols rapidly become obsolete in this accelerating digital world. Organizations that seek to position themselves most effectively for the next five years will need to take a relentless and proactive approach to building over-the-horizon defensive capabilities.

Jim Boehm is a partner in McKinsey's Washington, DC, office; **Charlie Lewis** is an associate partner in the Stamford office; and **Kathleen Li** is a specialist in the New York office, where **Daniel Wallance** is an associate partner. **Dennis Dias** is a senior adviser of McKinsey.

Designed by McKinsey Global Publishing