McKinsey & Company

Risk Practice

COVID-19 crisis shifts cybersecurity priorities and budgets

Cybersecurity technology and service providers are shifting priorities to support current needs: business continuity, remote work, and planning for transition to the next normal.

by Venky Anant, Jeffrey Caso, and Andreas Schwarz

July 2020

Few corporate functions shifted priorities so much and so quickly when the COVID-19 crisis struck as corporate cybersecurity operations and the technology providers that support them did. As legions of employees suddenly found themselves in a work-from-home model, chief information-security officers (CISOs) adjusted, pivoting from working on routine tasks and toward long-term goals to establishing secure connections for newly minted remote workforces. CISOs also took steps to prevent new network threats that target remote workers and to bolster business-facing operations and e-commerce after a surge in online shopping during pandemic lockdowns.

The response to the crisis continues to press department budgets and limit resources for other, less essential functions—a situation that we believe will direct spending in fiscal year 2021, which many departments are beginning to plan for. According to new McKinsey research, overall spending should taper off from the sector's recent rapid growth in industries that were hit hard by the COVID-19 crisis while holding steady in industries that have not been as affected.

The challenges that cybersecurity organizations face have spilled over to technology providers. Those companies have done their own pivots to keep up with customers' shifting needs and to institute new ways of doing business. To succeed in the post-COVID-19 era, technology providers must rethink their strategies and offerings to accommodate a new security landscape. And they must continue to monitor customers' needs and adjust sales, service, and training accordingly.

COVID-19 crisis's impact on cybersecurity spending

CISOs responded to the pandemic by quickly instituting measures to maintain business continuity and protect against new cyberthreats. To manage continuity, they have been patching remote systems over virtual private networks (VPNs) that have strained under increased loads. They have been monitoring spiking threat levels, including a near-sevenfold increase in spear-phishing attacks, since the pandemic began. Remote workers are also being bombarded with attacks based on COVID-19-crisis themes that are taking advantage of delayed updates to email and web filters, and using social engineering to prey on workforce concerns.

Many CISOs' fiscal 2020 budgets had already been allocated before the pandemic, so to cover the cost of addressing the crisis, they had to put other projects on hold. According to our research, which covers more than 250 global CISOs and security professionals, the crisis-inspired security measures will remain top budget priorities in the third and fourth quarters of 2020.

More than 70 percent of security executives also believe that their budgets for fiscal year 2021 will shrink, according to the survey. As a result, supporting new tactics to safeguard organizations is expected to limit outlays for such things as compliance, governance, and risk tools. For corporate security-operations centers, the cost of securing the fundamentals could reduce budgets for more advanced threat-intelligence upgrades, behavioral analytics, and other tooling.

In our client work, we have seen those priorities play out in many ways, including the following:

— A software company rerouted resources that had been designated for a security-automation project to cover gaps in multifactor authentication (MFA).

— A consumer-packaged-goods company postponed holding cybersecurity "war games" and diverted the resources to accelerate the rollout of a VPN.

— A financial-services company postponed "red team" exercises to close vulnerabilities in remote-work applications.

>70%

of CISOs and security buyers believe budgets will shrink by the end of 2020 but plan to ask for significant increases in 2021.

— In the next 12 months, spending will vary by industry (exhibit). For financial-services and insurance industries, for example, we expect to see budget increases for specific segments, such as security controls for the cloud-based business functions that more of those companies are adopting.

Our research suggests that other industries will not fare as well. Spending for healthcare payers should track with precrisis allocations but could taper off in the last half of the fiscal year because of budget constraints. Healthcare providers that have been on the front line of the crisis have had to adjust operations to interact with patients digitally and virtually, including through telemedicine. Implementing those new technologies have dug into operations budgets, and such companies could cut back on cybersecurity spending as a result.

We also expect retail companies' cybersecurity budgets to contract in line with lost revenues. However, an increase in online shopping means that some retailers are prioritizing investments in security for digital-payment platforms to support the evolving needs of their customers.

In most cases, we expect cybersecurity spending at large enterprises to bounce back faster than that at small and medium-size enterprises (SMEs).

Spending hot spots

Many companies are giving some or all employees the option of working remotely on a long-term or permanent basis. We expect other companies to reopen their physical offices in waves, welcoming back essential workers first, then other employees, and finally contractors, vendors, and other third parties. For industries that must maintain a sterile environment, such as healthcare, the process of returning nonessential people to the office could stretch even longer.

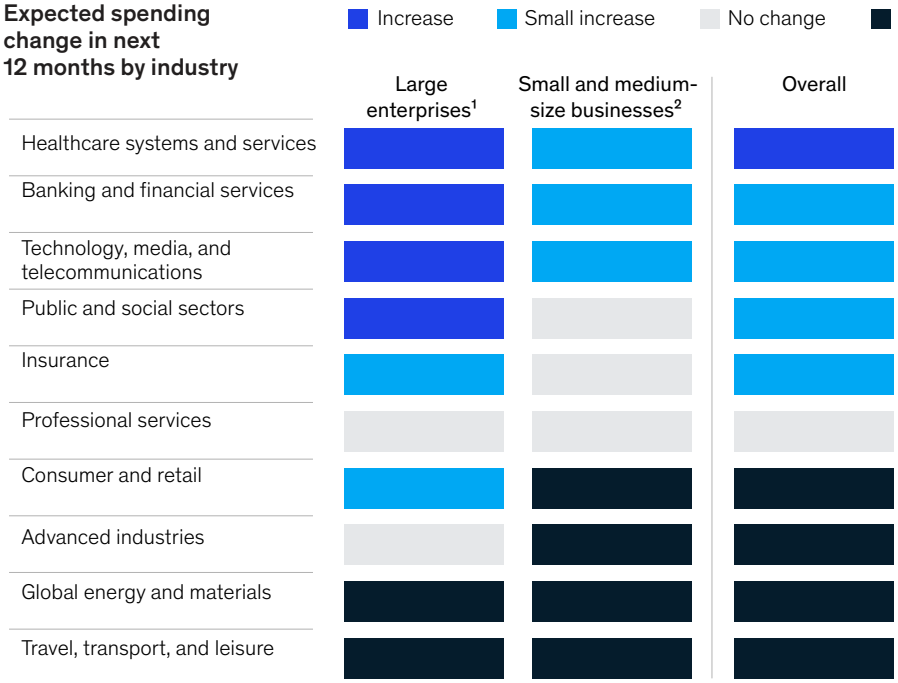
Based on those trends, other recent activity, and insights gleaned from our research, we believe CISOs and cybersecurity-operations teams will continue to make the following security niches high priorities for spending:

— *Perimeter security.* Companies will continue to prioritize short-term spending on security for remote workers. We also expect them to spend on e-commerce security that can be scaled to cover increased activity (including the SMEs that use third parties to provide such services). That could result in higher spending on pay-per-seat and pay-per-megabyte licenses and ultimately cause companies to shift additional funds from in-house systems to outsourced services.

Exhibit

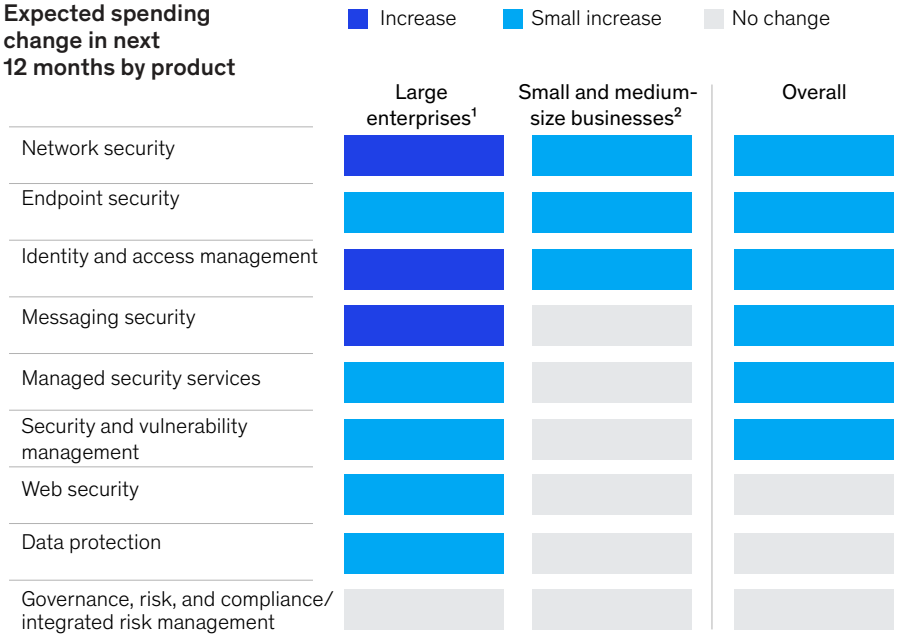
The COVID-19 crisis is expected to shift cybersecurity spending by industry and product category.

Expected spending change in next 12 months by industry



- Industries hardest hit by pandemic (eg, retail, energy) expect budgets to drop; small businesses will be more affected than large ones will
- Vendors could use customers' need for new services to recommend shifting cybersecurity tech stack to cloud rather than patching new features onto legacy systems

Expected spending change in next 12 months by product



- >70% of CISOs[3] and security buyers believe budgets will shrink by end of 2020 but plan to ask for significant increases in 2021
- Product spending reflects CISOs' need to address pandemic-era business conditions, including safeguarding remote workers from heightened attacks

[1]>5,000 employees.
[2]<5,000 employees.
[3]Chief information-security officers.
Source: Expert interviews; McKinsey analysis

— *Next-generation identity and access controls.* Companies that had deferred adding MFA to legacy systems are accelerating its adoption or are moving to cloud platforms. With more employees working remotely, teams managing business-critical systems are revisiting who qualifies for privileged access. CISOs at medium-size companies are likely to prioritize managing privileged-access and identity-governance solutions that integrate with security-information and event-management tools and with advanced security analytics to save time and money.

— *Remote access.* CISOs will continue to support virtual work-arounds for help-desk staff who would work in the office under normal circumstances. A virtual security help desk assists remote workers with access issues that also support productivity, such as email security tokens and remote desktop access. At SMEs in particular, we expect to see higher than average spending on MFA services that integrate with collaboration tools and system-as-a-service solutions, including file sharing, virtual-desktop infrastructure, and communication platforms.

— *Automation.* Companies that can automate routine tasks can free up time for other work that adds more value. At organizations that use outsourced services, we expect CISOs to ask managed-service providers to make up for increased workloads by adding such automated services as security orchestration automation and response tooling rather than by increasing staff or budgets.

— *Security training.* The crisis has provided companies with an opportunity to drive home cybersecurity's importance to the workforce, especially frontline employees. We expect that the cyberawareness training—that developed in-house and that delivered by an outside provider—that CISOs offer will be adapted both to cover remote-work situations and bring-your-own-device policies and to be delivered virtually.

— *Security for trusted third parties.* Companies that provide network access to contractors or other trusted partners need to protect those parties from outside attacks, since such threats could affect their own security. We expect to see companies increase monitoring for potential threats, which could increase budgets for click-of-a-button security-ratings tools, security-risk assessments, and security-reporting instruments—however, these expenses will not likely be prioritized until after any technical security gaps made more relevant by COVID-19 (for example, remote access security, multifactor authentication) have been closed.

Next normal for cybersecurity providers

Companies' actions to maintain business continuity and protect remote workers will likely have ramifications for cybersecurity providers over the 12 to 18 months (the time that CISOs estimate it will take for security organizations to reach the next normal). Plans for permanent remote work, phased reopening, and limited interaction with nonessential visitors will boost interest in some cybersecurity products and services but curb it for others. That will change how providers need to interact with customers and prospects:

— *Product refreshes could decrease.* To address budget constraints, CISOs are considering extending how long they use security applications before upgrading, especially for hardware-based services (such as firewalls). They also will prioritize paying for new features or patches for only the most critical applications. That could make organizations more vulnerable to attacks on their technology stacks, creating a business opportunity for providers to offer additional or new technologies or services.

— *Go-to-market touchpoints will shift.* Until regions reopen completely, providers' sales and marketing representatives can't meet face to face with security-team personnel. The nimblest will find other ways to keep in touch and provide extra value, such as by switching to video calls and using a customer-engagement application to record touchpoints.

— *Delivering services will be more challenging.* Providers won't be able to send technicians or other staff to a customer's facility to install or run an outsourced service, respond to a crisis, or help with a transformation project. In that absence, we forecast that demand for remote services and permissions under restricted access will increase.

— *The market for security and training will grow.* With cyberthreats to remote workers increasing, companies are motivated to boost training to improve awareness and educate them about cyber hygiene. Providers that can offer such services should be prepared to deliver them virtually, including for real-time interventions.

— *Customers may be open to replatforming.* CISOs that need to bring services in line with current needs may be more inclined to move those applications to new platforms, including the cloud. It may be easier to add MFA and single-sign-on features on modern cloud platforms than to bolt those features onto an older platform. If that's the case, rip-and-replace scenarios could present providers with an opportunity to negotiate new deals, especially if they can reduce cyberfriction and disruptions.

— *Short-term pricing strategies could open doors.* CISOs faced with budget pressures may need to revisit cybersecurity-services contracts to maximize value and cut costs. If providers are able, they could use the opportunity to extend licenses for a period of time without negative financial consequences to customers. That could solidify relationships while setting the stage for future contract extensions or renegotiations.

What cybersecurity providers can do

In the short term, we expect CISOs to continue to prioritize situations related to remote work and business continuity. But eventually, we expect the emergence of a phase of hybrid activity—one in which CISOs both take care of their immediate needs and begin to resume limited support for longer-term or strategic cybersecurity imperatives.

Providers can use this period of time to solidify existing relationships and build new ones as trusted partners and influencers. To get there, we recommend providers focus on the following key areas:

— *Anticipate customers' needs.* Understand the issues that security teams face to determine which products and services could best meet their needs. Security teams will be focused on supporting technology and security features—capabilities and services that are critical to their organizations' operations. Those needs will vary by team. An end-point-security team, for example, might focus on bring-your-own-device issues, and a network-security team may need to deal with VPN load to support a workforce split between working from the office and working from home. Similarly, needs may vary by company. A large insurance company might need to prioritize General Data Protection Regulation compliance as it accelerates the move of its business systems to the cloud, and a midsize utility might need to focus on network segmentation.

— *Adjust approaches and technologies to address urgent problems.* Develop a pitch that links an organization's mission statement to the issues that its customers are currently facing. If the

business case is right, look at opportunities to expand beyond the company's traditional wheelhouse through acquisition or in-house development of new capabilities. Opportunities to expand should sync with the areas in which CISOs are accelerating their own road maps, particularly maintaining security operations, mitigating the risk of remote access to sensitive data and software-development environments, and implementing MFA to enable employees to continue working remotely.

— *Assess the portfolio.* Times have changed. The solutions that a customer needs today may be different from when a provider first developed its portfolio, and it may need to shift its offerings as a result. After evaluating which products or services are likely to be more attractive in the recovery and next normal, providers can reorient engineering, sales, and marketing resources to support them. Play up the most compelling aspects of an integrated offering. If it is unclear that proprietary technology will continue to dominate a specific niche, it could be an opportunity to help customers optimize cybersecurity expenditures by suggesting open-source frameworks and solutions.

— *Invest in relationships.* When customers look back on this era, they will remember the partners that stuck with them. When providers can't build revenue, they can build relationships. Companies will continue to adjust security models to the requirements of different markets and regulators, and providers can help them by offering guidance and best practices.

CISOs that acted quickly to reorient security to cover remote workers and business continuity during the COVID-19 crisis must now prepare for the future. Such preparation includes determining how to allocate limited cybersecurity budgets to support additional modifications. Cybersecurity providers must shift their approaches, becoming trusted partners and influencers to help customers maximize their spending while preparing for the next normal.

Venky Anant is a partner in McKinsey's Silicon Valley office; **Jeffrey Caso** is an expert in the Washington, DC, office; and **Andreas Schwarz** is an expert in the New York office.

Designed by Global Editorial Services