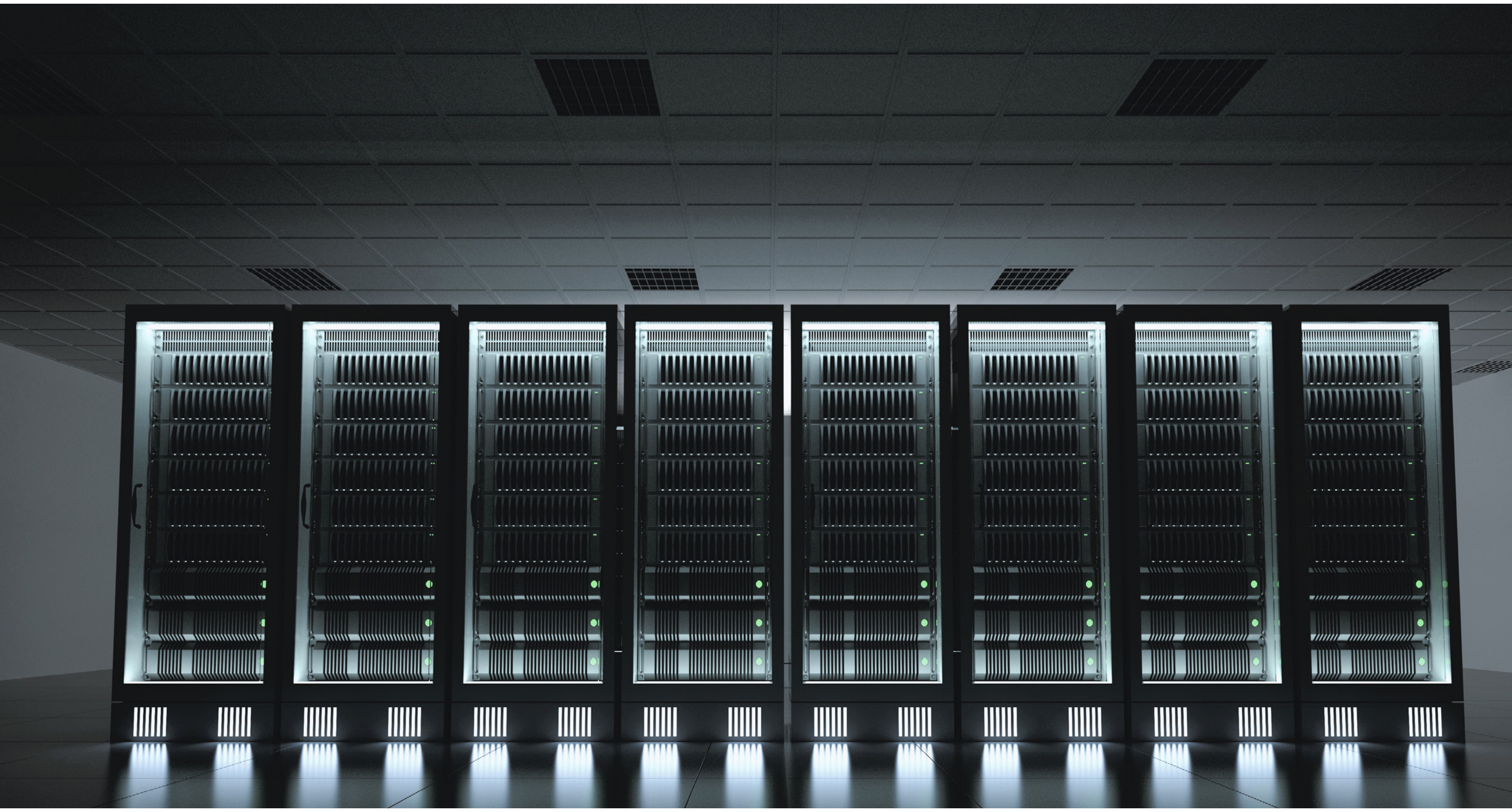
McKinsey & Company

Risk Practice

Cybersecurity's dual mission during the coronavirus crisis

Chief information-security officers must balance two priorities to respond to the pandemic: protecting against new cyberthreats and maintaining business continuity. Four strategic principles can help.

by Jim Boehm, James Kaplan, and Nathan Sportsman



© Fabian Schmidt/EyeEm/Getty Images

March 2020

The extraordinary efforts of many organizations to protect workers and serve customers during the COVID-19 pandemic have also increased their exposure to cyberthreats. 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 cyberattackers have been quick to exploit.

The overarching challenge for chief information-security officers (CISOs) and cybersecurity teams will be protecting their institutions while enabling operations to go on without interruption. For example, cybersecurity teams at companies that provide web-based services to consumers must adjust their security programs to match scaled-up operations while securing a massive shift to work-from-home tools. At the same time, CISOs must make it possible for security-team members to look after themselves and their families during a health crisis.

Addressing these diverse and sometimes competing needs at once won't be easy. But recent conversations with cybersecurity leaders suggest that some governing principles are helping them meet the challenge. This article recommends four such principles: focusing on critical operating needs, testing plans for managing security and technology risks, monitoring for new cyberthreats, and balancing protection with business continuity.

How the response to COVID-19 has increased cyberrisk

As organizations and people have curtailed travel and in-person gatherings, they have shifted a great deal of activity into the digital realm. Workers and students are staying home, using videoconferencing services, collaboration platforms, and other digital tools to do business and schoolwork. In their free time, they are going online to shop, read, chat, play, and stream. All these behaviors put immense stress on cybersecurity controls and operations. Several major vulnerabilities stand out:

— *Working from home has opened multiple vectors for cyberattacks.* A broad shift toward work-from-home arrangements has amplified long-standing cybersecurity challenges: unsecured data transmissions by people who aren't using VPN software, weak enforcement of risk-mitigating behaviors (the "human firewall"), and physical and psychological stressors that compel employees to bypass controls for the sake of getting things done. The more that homebound employees struggle to access data and systems, the more they will attempt to use risky work-arounds (exhibit). Cybersecurity teams will need to secure work-from-home systems and test and scale VPNs and incident-response tools. In addition, they may wish to revisit access-management policies so that employees can connect to critical infrastructure via personal devices or open, internet-facing channels.

— *Social-engineering ploys are on the rise.* In social-engineering gambits, attackers attempt to gain information, money, or access to protected systems by tricking legitimate users. Companies have seen more malware-laced email-phishing campaigns that borrow the identities of health, aid, and other benevolent organizations. Scammers posing as corporate help-desk teams ask workers for their security credentials using text phishing ("smishing") and voice phishing ("vishing"). Email fraudsters have tried to get executives to move money to fund vendors, operations, and virus-related-response activities.

— *Cyberattackers are using websites with weak security to deliver malware.* With the creation of new domains and websites to spread information and resources to combat the coronavirus, attackers are exploiting the weak security controls on many of these sites to spread malware via drive-by downloads. A common approach hides readily available malware (such as AZORult) inside coronavirus heat maps or early-warning applications. In one

Exhibit

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 (eg, data infiltration, data-protection loss), from less critical apps accessible from almost anywhere (eg, public network) to apps accessible through extranet, apps accessible only through VPN, and, ultimately, critical apps accessible only on site (eg, 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

instance, a threat actor targeted a public-sector entity by embedding malware in a pandemic-related document and disguising it as an official communiqué from another part of the government. Once installed, such a malicious application steals a user's confidential data (for example, personal information, credit-card information, and bitcoin-wallet keys). Some malware applications launch ransomware attacks, which lock a user's system until they pay a certain amount of money to the attacker.

— *Public-sector organizations are experiencing acute pressure.* A large government entity in North America suffered from a distributed denial-of-service attack aimed at disrupting services and issuing misinformation to the public. A major hospital in Europe was hit with a cyberattack that forced it to suspend scheduled operations, shut down its IT network, and move acute-care patients to another facility. And a department of a local government had its website encrypted by ransomware, preventing officials from posting information for the public and keeping employees from accessing certain files.

As the COVID-19 outbreak progresses and alters the functioning of our socioeconomic systems, cyberattackers will continue their efforts to exploit our fears and our digital vulnerabilities. To remain vigilant and effective, CISOs will need new approaches.

Employees on the front line will play an especially important role in keeping the organization safe as normal on-premise security measures become less relevant.

How to address the challenge: Strategic practices for chief information-security officers

While many CISOs and other executives have drawn on their experiences with past crises to respond to the early stages of the COVID-19 outbreak, the pandemic's vast scale and unpredictable duration are highly unusual. There is no playbook that CISOs can open for guidance. Nevertheless, the CISOs and senior cybersecurity managers we have spoken to have found it especially helpful to follow four practices:

- *Focus.* Security- and technology-risk teams should focus on supporting only those technology and security features, capabilities, and service rollouts that are critical to operations. Examples of focus areas that may justify a surge in capacity over the coming weeks include maintaining security operations, mitigating risks of remote access to sensitive data and software-development environments, and implementing multifactor authentication to enable employees to work from home. Organizations should also reiterate to employees their safe remote-working protocols and their procedures for threat identification and escalation. Employees on the front line will play an especially important role in keeping the organization safe as normal on-premise security measures become less relevant.

- *Test.* If your organization has security- or technology-risk plans of any kind—such as plans for incident response, business continuity, disaster recovery, talent succession, and vendor succession—then test them right away. If your organization doesn't have adequate plans in place, create them and then test them. You must determine whether your organization's risk-response approach is effective and efficient. Eliminating risk events is impossible, but you can reduce the exacerbated risk associated with a poor response.

- *Monitor.* Consider mustering all available resources to help with monitoring, which enables risk response and recovery to begin. Areas for stepped-up monitoring can include remote monitoring of collaboration tools, monitoring networks for new and novel strains of malware, and monitoring employees and endpoints to catch data-related incidents before they result in operational risk.

- *Balance.* Cybersecurity teams are likely to receive a flood of urgent requests for cybersecurity-policy exceptions that will allow teams elsewhere in the organization to get work done (for example, to approve the installation of new apps and allow the use of USB drives). While CISOs might be inclined to deny such requests for the sake of preventing undue risk, they must also bear in mind the importance of maintaining business continuity during a fluid and challenging time for their colleagues. To support continued operations, CISOs may need to tolerate slightly higher risk in the short term by granting waivers or temporarily relaxing some controls. An accommodating approach will encourage colleagues to make intelligent risk trade-offs. That said, CISOs shouldn't allow these exceptions to weaken an organization's risk posture permanently. If CISOs grant waivers or relax controls, they should establish formal evaluation and review processes and implement time limits to force periodic reevaluation or limit the exceptions to particular user groups.

The COVID-19 crisis is a human challenge above all else. Everyone is juggling professional responsibilities with important personal ones. The coming weeks and months are likely to bring more uncertainty. By adhering to the practices we described—focus, test, monitor, and balance—CISOs can fulfill their responsibilities to uphold their institutions' security and maintain business continuity while also meeting their obligations to their teams.

Jim Boehm is a partner in McKinsey's Washington, DC, office; **James Kaplan** is a partner in the New York office; and **Nathan Sportsman** is the founder and CEO of Praetorian.

McKinsey and Praetorian have entered into a strategic alliance to help clients solve complex cybersecurity challenges and promote innovation. As a part of this alliance, McKinsey is a minority investor in Praetorian.

Designed by Global Editorial Services