McKinsey & Company

Risk Practice

Cybersecurity tactics for the coronavirus pandemic

The pandemic has made it harder for companies to maintain security and business continuity. But new tactics can help cybersecurity leaders to safeguard their organizations.

by Jim Boehm, James Kaplan, Marc Sorel, Nathan Sportsman, and Trevor Steen

© Gorodenkoff/Getty Images

March 2020

The COVID-19 pandemic has presented chief information security officers (CISOs) and their teams with two immediate priorities. One is securing work-from-home arrangements on an unprecedented scale now that organizations have told employees to stop traveling and gathering, and government officials in many places have advised or ordered their people to stay home as much as possible. 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 especially helpful to fulfill these two priorities. In this article, we set out the technology modifications, employee-engagement approaches, and process changes that cybersecurity leaders have found effective.

Securing work-from-home arrangements at scale

The rapid, widespread adoption of work-from-home tools has put considerable strain on security teams, which must safeguard these tools without making it hard or impossible for employees to work. Conversations with CISOs in Asia, Europe, and North America about how they are securing these new work-at-home arrangements highlight the changes these executives are making in three areas: technology, people, and processes.

Technology: Make sure required controls are in place

As companies roll out the technologies that enable employees to work from home and maintain business continuity, cybersecurity teams can take these actions to mitigate cybersecurity risks:

- *Accelerate patching for critical systems.* Shortening patch cycles for systems, such as virtual private networks (VPNs), end-point protection, and cloud interfaces, that are essential for remote working will help companies eliminate vulnerabilities soon after their discovery. Patches that protect remote infrastructure deserve particular attention.
- *Scale up multifactor authentication.* Employees working remotely should be required to use multifactor authentication (MFA) to access networks and critical applications. Scaling up MFA can be challenging: the protection it will add calls for a surge in short-term capacity. Several practices make the rollout of MFA more manageable. One is to prioritize users who have elevated privileges (such as domain and sys admins, and application developers) and work with critical systems (for instance, money transfers). Targeting those users in pilot rollouts of modest scale will allow cybersecurity teams to learn from the experience and use that knowledge to shape more extensive implementation plans. Cybersecurity teams can also benefit from using MFA technologies, such as the application gateways offered by several cloud providers, that are already integrated with existing processes.
- *Install compensating controls for facility-based applications migrated to remote access.* Some applications, such as bank-teller interfaces and cell-center wikis, are available only to users working onsite at their organizations' facilities. To make such facility-based applications available to remote workers, companies must protect those apps with special controls. For example, companies might require employees to activate VPNs and use MFA to reach what would otherwise be facility-based assets while permitting them to use MFA alone when accessing other parts of the corporate environment.
- *Account for shadow IT.* At many companies, employees use so-called shadow IT systems, which they set up and administer without formal approval or support from the IT department. Extended work-from-home operations will

expose such systems because business processes that depend on shadow IT in the office will break down once employees find themselves unable to access those resources. IT and security teams should be prepared to transition, support, and protect business-critical shadow assets. They should also keep an eye out for new shadow-IT systems that employees use or create to ease working from home, to compensate for in-office capabilities they can't access, or to get around obstacles.

— *Quicken device virtualization.* Cloud-based virtualized desktop solutions can make it easier for staff to work from home because many of them can be implemented more quickly than on-premises solutions. Bear in mind that the new solutions will need strong authentication protocols—for example, a complex password, combined with a second authentication factor.

People: Help employees understand the risks
Even with stronger technology controls, employees working from home must still exercise good judgment to maintain information security. The added stress many people feel can make them more prone to social-engineering attacks. Some employees may notice that their behavior isn't monitored as it is in the office and therefore choose to engage in practices that open them to other threats, such as visiting malicious websites that office networks block. Building a "human firewall" will help ensure that employees who work from home do their part to keep the enterprise secure.

— *Communicate creatively.* A high volume of crisis-related communications can easily drown out warnings of cybersecurity risks. Security teams will need to use a mix of approaches to get their messages across. These might include setting up two-way communication channels that let users post and review questions, report incidents in real time, and share best practices; posting announcements to pop-up or universal-lock screens; and encouraging the innovative use of existing communication tools that compensate for the loss of informal interactions in hallways, break rooms, and other office settings.

— *Focus on what to do rather than what not to do.* Telling employees not to use tools (such as consumer web services) they believe they need to do their jobs is counterproductive. Instead, security teams must explain the benefits, such as security and productivity, of using approved messaging, file-transfer, and document-management tools to do their jobs. To further encourage safe behavior, security teams can promote the use of approved devices—for example, by providing stipends to purchase approved hardware and software.

— *Increase awareness of social engineering.* COVID-19–themed phishing, vishing (voice phishing), and smishing (text phishing) campaigns have surged. Security teams must prepare employees to avoid being tricked. These teams should not only notify users that attackers will exploit their fear, stress, and uncertainty but also consider shifting to crisis-specific testing themes for phishing, vishing, and smishing campaigns.

— *Identify and monitor high-risk user groups.* Some users, such as those working with personally identifiable information or other confidential data, pose more risk than others. High-risk users should be identified and monitored for behavior (such as unusual bandwidth patterns or bulk downloads of enterprise data) that can indicate security breaches.

Processes: Promote resilience
Few business processes are designed to support extensive work from home, so most lack the right embedded controls. For example, an employee who has never done high-risk remote work and hasn't set up a VPN might find it impossible to do so because of the in-person VPN-initiation requirements. In such cases, complementary security-control processes can mitigate risks. Such security processes include these:

Even with stronger technology controls, employees working from home must still exercise good judgment to maintain information security.

- *Supporting secure remote-working tools.* Security and IT help desks should add capacity while exceptionally large numbers of employees are installing and setting up basic security tools, such as VPNs and MFA. It might be practical to deploy security-team members temporarily at call centers to provide added frontline support.

- *Testing and adjusting IR and BC/DR capabilities.* Even with increased traffic, validating remote communications and collaboration tools allows companies to support incident-response (IR) and business-continuity (BC)/disaster-recovery (DR) plans. But companies might have to adjust their plans to cover scenarios relevant to the current crisis. To find weak points in your plans, conduct a short IR or BC/DR tabletop exercise with no one in the office.

- *Securing physical documents.* In the office, employees often have ready access to digital document-sharing mechanisms, as well as shredders and secure disposal bins for printed materials. At home, where employees might lack the same resources, sensitive information can end up in the trash. Set norms for the retention and destruction of physical copies, even if that means waiting until the organization resumes business as usual.

- *Expand monitoring.* Widening the scope of organization-wide monitoring activities, particularly for data and end points, is important for two reasons. First, cyberattacks have proliferated. Second, basic boundary-protection mechanisms, such as proxies, web gateways, or network intrusion-detection systems (IDS) or intrusion-prevention systems (IPS), won't secure users working from home, off the enterprise network, and not connected to a VPN. Depending on the security stack, organizations that do not require the use of a VPN or require it only to access a limited set of resources may go largely unprotected. To expand monitoring, security teams should update security-information-and-event-management (SIEM) systems with new rule sets and discovered hashes for novel malware. They should also increase staffing in the security operations center (SOC) to help compensate for the loss of network-based security capabilities, such as end-point protections of noncompany assets. If network-based security capabilities are found to be degraded, teams should expand their IR and BC/DR plans accordingly.

- *Clarify incident-response protocols.* When cybersecurity incidents take place, SOC teams must know how to report them. Cybersecurity leaders should build redundancy options into response protocols so that responses don't stall if decision makers can't be reached or normal escalation pathways are interrupted because people are working from home.

— *Confirm the security of third parties.* Nearly every organization uses contractors and off-site vendors, and most integrate IT systems and share data with both contract and noncontract third parties, such as tax or law-enforcement authorities. When organizations assess which controls must be extended to employees to secure new work-from-home protocols, they should do the same for third-party users and connections, who are likely to be managing similar shifts in their operations and security protocols. For example, ask providers whether they have conducted any remote IR or BC/DR tabletop drills and, if they have, ask them to share the results. Should any third parties fail to demonstrate adequate security controls and procedures, consider limiting or even suspending their connectivity until they remediate their weaknesses.

— *Sustain good procurement practices.* Fast-track procurement intended to close key security gaps related to work-from-home arrangements should follow standard due-diligence processes. The need for certain security and IT tools may seem urgent, but poor vendor selection or hasty deployment could do more harm than good.

Supporting high levels of consumer-facing network traffic

Levels of online activity that challenge the confidentiality, integrity, and availability (CIA) of network traffic are accelerating. Whether your organization provides connectivity, serves consumers, or supports transactions, securing the CIA of network activity should be a top priority for any executive team that wants to protect consumers from cyberbreaches during this period of heightened vulnerability. Much as organizations are stepping up internal protections for enterprise networks, security teams in organizations that manage consumer-facing networks and the associated technologies will need to scale up their technological capabilities and amend processes quickly.

Technology: Ensure sufficient capacity

Companies that make it possible for employees to work from home must enable higher online network-traffic and transaction volumes by putting in place technical building blocks such as a web-application firewall, secure-sockets-layer (SSL) certification, network monitoring, antidistributed denial of service, and fraud analytics. As web-facing traffic grows, organizations should take additional actions to minimize cyberrisks:

— *Enhance web-facing threat-intelligence monitoring.* To anticipate threats and take preventive measures, security teams must understand how heightened consumer traffic changes the threat environment for web-facing enterprise activities. For example, to find out if attackers are becoming more interested in an organization's web-facing technologies, organizations can conduct increased passive domain-name scans to test for new malicious signatures tailored to the enterprise domain or for the number of adversarial scans targeting the enterprise network, among other threats.

— *Improve capacity management.* Overextended web-facing technologies are harder to monitor and more susceptible to attacks. Security teams can monitor the performance of applications to identify suspected malware or low-value security agents or even recommend the removal of features (such as noncritical functions or graphics on customer portals) that hog network capacity.

Processes: Integrate and standardize security activities

Customers, employees, and vendors all play some part in maintaining the confidentiality, integrity, and availability of web-facing networks. Several steps can help organizations to ensure that the activities of these stakeholders are consistent and well integrated:

— *Integrate fraud-prevention capabilities with the SOC.* Organizations that support the execution of financial transactions should consider integrating their existing fraud analytics with

SOC workflows to accelerate the inspection and remediation of fraudulent transactions.

- *Account for increased costs.* Many SOC tools and managed-security-service providers base charges for monitoring on usage—for example, the volume of log records analyzed. As usage increases with expanded network traffic, organizations with usage-based fee arrangements will need to account for any corresponding increase in costs.

- *Help consumers solve CIA problems themselves.* For media providers, enabling customers to access content without interruption is essential, but increased usage levels can jeopardize availability. Companies may wish to offer guides to show users how to mitigate access problems, particularly during periods of peak use.

Securing remote-working arrangements and sustaining the CIA of customer-facing networks are essential to ensure the continuity of operations during this disruptive time. The actions we describe in this article, while not comprehensive, have helped many organizations to overcome the security difficulties they face and maintain their standing with customers and other stakeholders.

Jim Boehm is a partner in McKinsey's Washington, DC, office; **James Kaplan** is a partner in the New York office; and **Marc Sorel** is a partner in the Boston office. **Nathan Sportsman** is the founder and CEO of Praetorian, where **Trevor Steen** is a senior security engineer.

The authors wish to thank Wolf Richter and Mahir Nayfeh for their contributions to this article.

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

Designed by Global Editorial Services