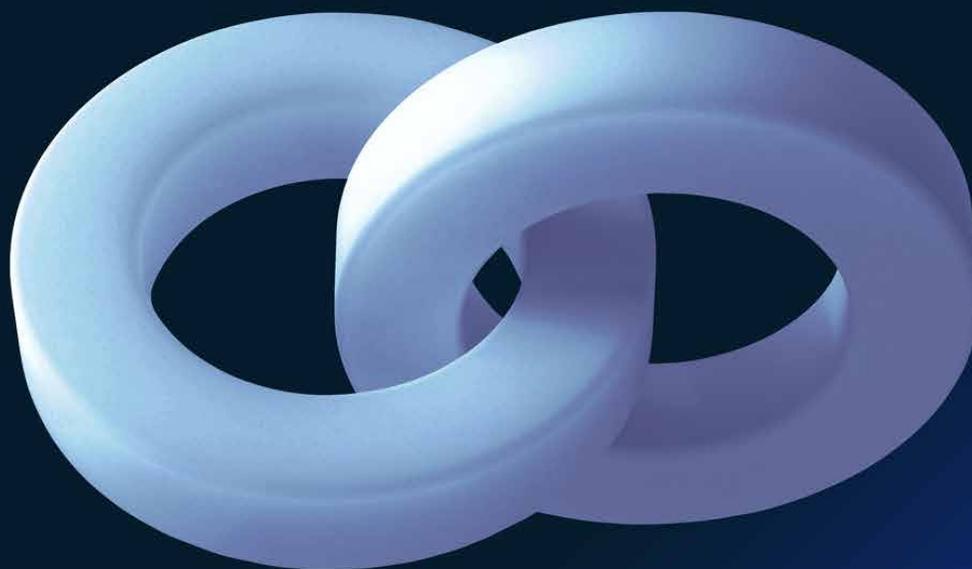


Risk Practice

A dual cybersecurity mindset for the next normal

As companies extend commitments to remote workforces, cybersecurity teams need to address new risks while helping create business value in the next normal.

by Venky Anant, Soumya Banerjee, Jim Boehm, and Kathleen Li



As the COVID-19 pandemic swept across the world, most organizations made a quick transition to a remote workforce and a more intense focus on serving customers through digital channels. This created a rapid surge in demand for digital capabilities, products, and services. Cybersecurity teams, for their part, were largely successful in taking on a dual mission of supporting business continuity and protecting the enterprise and its customers.

The digital response to the COVID-19 crisis has also created new security vulnerabilities. Attackers seek to exploit the gaps opened when telecommuting employees use insecure devices and networks. Threat actors also use known attack techniques to exploit people's COVID-19-related fears. For example, Google tallied more than 18 million malware and phishing emails related to the novel coronavirus on its service each day in April. It also reported identifying more than a dozen government-backed groups using COVID-19 themes for these attempts.¹

The COVID-19 pandemic and the efforts to contain it have had serious economic and business consequences. These are affecting core dimensions of the business environment, from digital strategies to operational and enterprise risk appetite. Supply-chain configuration and business interactions with regulators are likewise being reshaped, as are the ways we think about the very nature of work. A McKinsey survey of digital sentiment revealed that most employees who are now telecommuting do not expect to return to the workplace soon. Seventy percent of those responding believe that the ability to continue telecommuting will factor into their next job choice.² Customers express similar sentiments: 75 percent of respondents using digital channels as a result of the COVID-19 crisis say that they will continue to do so.³

Chief information-security officers (CISOs) and cybersecurity teams will need to approach the next horizon of business with a dual mindset. They must

first address the new risks arising from the shift to a remote digital working environment, securing the required technology. They will also need to anticipate the next normal—how their workforce, customers, supply chain, channel partners, and sector peers will work together—so that they may appropriately engage and embed security by design. The new context of changing customer and employee behavior and a constantly shifting threat landscape must also be considered.

The pandemic response has underscored the vital role that security plays in enabling remote operations, both during and after a crisis. As companies reimagine their processes and redesign architecture amid the COVID-19 response, cybersecurity teams are being perceived anew. They must no longer be seen as a barrier to growth but rather become recognized as strategic partners in technology and business decision making.

Addressing risks and fortifying gains

Throughout the crisis, cybersecurity leaders responded with a focus on three activities as companies shifted to new processes and technologies: assessing and knocking down hot spots, fixing and mopping up operations, and fortifying incremental digital gains. Efforts in each area occur simultaneously and are ongoing. Cybersecurity teams may only just be arriving at the point where they are fortifying initial incremental gains; they may also have to reevaluate prior efforts as new technologies or processes are introduced. Here are some of the experiences in these three areas companies and cybersecurity leaders have shared with us.

Assessing and knocking down hot spots

As employees began working from home in less secure environments and, in many cases, with less secure personal equipment, security teams have had to remediate immediate operational, process, and technology gaps related to the pandemic-induced response and the shift to remote working.

¹ *Threat Analysis Group*, "Findings on COVID-19 and online security threats," blog entry by Shane Huntley, Google, April 22, 2020, blog.google.

² "Costs and benefits," *Global Workplace Analytics*, globalworkplaceanalytics.com.

³ McKinsey COVID-19 US Digital Sentiment Survey, April 2020.

A financial-services company supported all of its call-center staff in working remotely and connecting securely by providing them with Wyse thin-client terminals.

Leaders have had to address training gaps, lead virtual all-hands meetings, and call on workers to maintain digital hygiene, such as patching their computers and updating mobile software.

For example, a large financial-services company was able to support its remote workforce swiftly by distributing Wyse thin-client terminals to all call-center staff for secure remote connections. Some initial issues with bandwidth and performance were resolved by performing virtual-private-network (VPN) split tunneling as well as upgrading firewall infrastructure. The company also enabled remote patching to all end-user devices by upgrading all its AnyConnect remote servers.

In another case, a large bank adjusted several security policies in response to the COVID-19 crisis. The company ran more frequent awareness campaigns (with tailored pandemic-themed content), resulting in a 95 percent improvement in employee click rates during monthly antiphishing tests. Additionally, the organization introduced restrictions on USB connections and put critical patches on a 30-day cycle.

Fixing and mopping up operations

In the early days of the pandemic response, many companies were forced to accept new risks, including reduced control standards, to keep operations going. As employees and

customers became accustomed to the changes, companies evaluated these residual risks and tightened controls.

For example, to catch up with a surge in adoption of various cloud-based collaboration tools, a large telecommunications provider accelerated the rollout of new cloud-aware monitoring capabilities within its security-incident and event-monitoring (SIEM) tool. Additionally, it reviewed its security and monitoring controls for third-party vendors to ensure that restrictions that had been temporarily lifted were put back in place.

Along the same lines, a large bank conducted threat modeling on its new collaboration tools that employees had been using, including unauthorized tools introduced during the shift to remote working. The bank also updated security controls or replaced products based on acceptable-risk thresholds.

Fortifying security gains

As employees became comfortable working from home, companies began standardizing procedures for remote work environments and explored technologies to reduce long-term risk.

Some companies introduced stronger consumer-security and fraud-prevention controls. A large bank expanded its biometric- and device-based

authentication for sensitive customer transactions across new, critical digital channels. The bank also accelerated implementation of a state-of-the-art, artificial-intelligence-based fraud-detection platform. As a result, incoming transactions could be analyzed in 300 milliseconds or less, compared with the hours this took before.

In another instance, a national insurance company updated policies and procedures to institutionalize the security controls required in a remote work environment. It established a new policy and standard to mitigate the risk of cybercriminals infiltrating the network through unsecured home printers. Except for approved business cases, all employees were restricted from printing remotely through personal printing devices.

Anticipating the next normal

As cybersecurity leaders are increasingly getting a handle on the first stage of the pandemic, CISOs are now shifting to anticipating how the business environment will be affected by new conditions. They are adapting to incorporate these expectations of the next normal into both current

cybersecurity activities and long-term cyber risk strategies (Exhibit 1).

Secure the workforce in new ways of working

The COVID-19 crisis has fundamentally changed ways of working, as many companies are extending the remote-working policies that became necessary during the pandemic (see sidebar “A case example on securing the workforce”). Organizations could emphasize the following cybersecurity initiatives:

- *Dynamic security.* Static, network-based security perimeters will no longer be sufficient. The security dynamic among users, assets, and resources must be the new focus. Define identity as a perimeter with scaled-up capabilities in identity and access management, privileged-access management, multifactor authentication (based on devices or biometrics), key management, and heuristics based on log-on behavior. For assets, consider a strategy using a software-defined perimeter and enhanced network segmentation (using logical microsegmentation through next-generation firewalls). Protect end-point assets and utilize real-time anomaly detection with end-point-

Exhibit 1

To secure the next-normal business environment for value creation and growth, cybersecurity leaders will need to take effective action in four priority areas.

Next-normal attributes

				
Actions to take	Secure workforce in new ways of working	Secure customer journey through digital shift	Rethink supply chain and third-party risk	Sustain increased sector collaboration
Key levers	<ul style="list-style-type: none"> • Dynamic security • Cloud-based tools and infrastructure • People defense • “Contact aware” workforce privacy • Remote cybersecurity operating model and talent strategy 	<ul style="list-style-type: none"> • Frictionless customer experience • At-scale digital channels • Privacy by design • Advanced analytics 	<ul style="list-style-type: none"> • Risk-tiered and expanded coverage • Updated third-party security assessment • Joint cyberresilience and monitoring • Secure partner collaboration • Plan for geopolitical challenges 	<ul style="list-style-type: none"> • Sustained increased sector-wide information sharing • Industry-level initiatives to reduce barriers and secure digital shift

An insurance company restricted all its employees from printing remotely through personal printing devices except for approved business cases.

detection and -response systems. Protect data assets through enhanced block-mode data-loss-prevention tools and utilize a model of preapproved sites as a default for external access.

- *Cloud-based tools and infrastructure.* The need for greater agility and flexibility will accelerate the use of the cloud. Restrict localized data storage for the remote workforce and transform end-user infrastructure through increased adoption of virtual desktop and desktop as a service. Support the increasing shift to a multicloud environment and cloud-based services through access controls at points

where policy is decided and enforced; implement a cloud-access-security broker.

- *'Contact aware' workforce privacy.* Heightened security will require new agreements with employees. Factor in the implications of workforce privacy and employee consent to introduce contact-aware tools, such as contact tracing and temperature taking, in the workplace (as enabled, for example, in the API for contact tracing that is integral to the recent iOS 13.5 update).
- *People defense.* Companies will need to extend their operational defenses as working

A case example on securing the workforce

A global bank believed it was impossible to exfiltrate sensitive information from its environment. A targeted test on end-point and data controls, however, found more than 70 security gaps, with a large number directly related to the remote work environment. The virtual private network's always-on design, for instance, had many loopholes that could be exploited. Weak two-factor control relied on personal identification numbers and passwords

rather than device, token, or biometric authentication. Data-transfer rules were in monitor mode instead of block mode, and internet-access rules were in "blacklist" mode (blocking suspicious sites) rather than allowing preapproved sites). In one instance, a customer's personally identifiable financial information was altered using a cypher, and more than 20,000 records were extracted without detection and blocking.

The following issues were discovered:

- More than 70 gaps were identified in the effectiveness and coverage of the security architecture, including prevention, detection, and mitigation capabilities.
- Despite the bank's belief that exfiltration of sensitive information from its environment was impossible, 16 ways to do so were discovered.

from home becomes standard. Roll out insider-threat-detection programs and explicit policies for a safe remote workplace. These could include restricted remote printing and prohibited sharing of company devices with family members. In addition, companies could consider helping employees manage stress levels, offering support in the current circumstances. Protecting employees is not just a leadership imperative: it will also reduce vulnerabilities created by worker anxiety.

- *Remote cybersecurity operating model and talent strategy.* The new ways of working will have implications across the enterprise. Rethink the cybersecurity operating model and continuity plans for physical-location-constrained operations, including automation opportunities. Derisk by design and further embed in application-development processes the principles and capabilities of DevSecOps—the linkage among development, security, and operations. Use the imperative of remote working as an opportunity to gain access to a broader pool of cybersecurity talent where there is an existing gap in local talent pools.

Secure the customer journey through the shift to digital business

Customers should be offered a secure and seamless digital experience—especially first-time users or those who are not tech savvy. As customers demand

greater choice in their interactions with companies and expect greater digital availability, cybersecurity teams can add value by helping their institutions reimagine the secure customer journey (see sidebar “A case example on securing the customer journey”). Several cybersecurity levers should be prioritized here:

- *Frictionless customer-security experience.* Advance capabilities on customer-identity and -access management, including the use of a single customer identity across all digital channels and of omnichannel authentication. These capabilities enable users to move a transaction among web, mobile, and call-center channels with minimal friction. Define customer personas, associated priorities, and potential pain points. Develop plans to address those pain points through customer-security design.
- *At scale.* Test cybersecurity controls (such as log-on controls, bot mitigation, network security, and firewalls) and monitoring to understand whether they can continue to perform at scale. Determine whether there is adequate redundancy in high-volume environments without adverse impact on user experience.
- *Privacy by design.* Treat customers as partners in security, involving them in an education and awareness campaign. High-value customers in need of greater tech awareness can be offered

A case example on securing the customer journey

An insurance company realized that providing a secure journey for customers required abandoning an internally developed customer-authentication solution. The solution was difficult for customers to use, often resulting in session time-outs during a transaction. One-time passwords took too long to get to customers during

peak hours, and a cumbersome application of security controls significantly increased friction. Key customers chose not to utilize this service at all.

The company developed the following approach:

- More than 50 in-scope security controls were identified as part of the customer journey.
- Nine new user personas were identified to enhance the customer security experience.

free antivirus and identity-monitoring services. Controls on customer-data usage and customer consent should also be applied. Develop plans to respond to and recover from customer-data breaches, and build them into the organization.

- *Advanced analytics.* Integrate security in fraud controls and vice versa. Feed security data (including log-on, device-binding, and jailbroken-device information) to heuristic risk-model engines that can improve authentication or stop a fraudulent transaction.

Rethink supply chain and third-party risk

Companies must consider third-party and channel-partner cybersecurity levels as carefully as they consider security policies for employees and customers. It is critical to assess supply-chain-continuity and -resilience controls against the permanent changes to ways of operating (see sidebar “A case example on securing the supply chain”). Organizations could emphasize the following actions:

- *Expand assessment coverage.* Expand assessment coverage to review all vendors and potential shadow third-party services—and not only those for IT services. Assign risk tiers to vendors, deciding which are most critical to operations and have the greatest access to vital information; calibrate assessment scope correspondingly.

- *Update controls for third-party-security controls and build joint cyberresilience.* Revise security-assessment controls for third parties to account for their remote operations. For example, companies could formulate vendor-continuity plans for offshore vendor centers that have physically restricted “clean rooms.” Such restrictions may disrupt operations when the vendor workforce has to work remotely. Where possible, integrate critical third-party logs into enterprise security monitoring and alert systems for coordinated monitoring and response.

- *Secure partner collaboration.* Secure remote-collaboration tools with partners. Take into account potential security implications in the business conditions of key partners. For example, a white-label credit-card partnership with a retail partner would be affected if the partner goes bankrupt. After bankruptcy, the white-label credit-card issuer may see increased incidents of insider threat or fraud.

- *Plan for geopolitical challenges.* Include geopolitical cybersecurity implications for critical vendor management, such as how countries may enforce full access to any data processed by a locally registered vendor.

Sustain increased sector collaboration

During the pandemic, peers and industry sectors collaborated in new ways, and companies worked with regulators to enable the transition to new

A case example on securing the supply chain

A global consumer-packaged-goods company determined that its cyber-risk-management processes for third parties were only being applied to vendors that were a part of the IT-procurement process. This exposed the organization

to cyberrisks presented by other types of vendors (for example, non-IT vendors, strategic partners, and acquisitions). Risk assessments were refreshed inconsistently or were nonexistent for many third parties, such as the ones that came

through acquisitions. The company discovered that half of its third-party vendors (10,000 in total) did not go through the IT procurement process and therefore did not complete third-party cybersecurity assessment.

ways of working. These partnerships must be strengthened to support processes that will change significantly after the pandemic. For example, the use of telemedicine has expanded exponentially during the pandemic and will likely reshape how healthcare is delivered. This will require companies to collaborate with regulators to formulate appropriate approaches to privacy and other regulatory-compliance requirements. The Industry Information Sharing and Analysis Center (ISAC) and other industry bodies are destined to play an even larger role in reducing the barriers to sharing information across companies and building joint resilience. The topic was explored in a recent survey on cyberresilience conducted by the Institute of International Finance and McKinsey.

Cybersecurity road map for the next normal

Organizations adopting a dual cybersecurity mindset will need flexibility in determining cybersecurity priorities according to business needs. Obviously, priorities will differ from sector to sector and company to company. For many companies, the economic slowdown caused by the crisis will restrict appetites to invest in cybersecurity; for the many others that have experienced a dramatic increase in online traffic during the pandemic, increased funding may be needed to secure new online channels at scale.

CISOs will have many different levers to apply and opportunities to consider, so they should plan their security strategies to best align with business strategies and priorities. These may have changed because of the pandemic. They can consider three factors in setting security plans: opportunities, parameters, and time frame.

- *Opportunities.* The cybersecurity opportunity will be determined by the transformation in the cyber risk appetite triggered by crisis-driven business change (such as remote work and

increased customer traffic). The cybersecurity team can anticipate and embed needed security capabilities, at the right level of maturity, by working with business partners. The business will help identify opportunities where the organization can leapfrog current security capabilities and set an optimal cyber pathway to support further business growth.

- *Parameters.* Companies will have to set limits, prioritizing essential security initiatives and connecting the priorities with available resources. Given the current operations and business environment, security teams will especially need to account for project capacity and underlying business economic conditions while prioritizing efforts. CISOs should agree with business stakeholders on the scope of critically needed cybersecurity initiatives and then work with business, finance, and IT partners to develop joint business cases to ensure rapid funding and completion.
- *Timing.* Cybersecurity leaders should clearly articulate time frames for all cyber efforts, balancing quick wins to reduce immediate operational risk with longer-term efforts that account for strategic shifts in the business portfolio. The cyber road map should align with business timelines and the pace of digitization.

Exhibit 2 shows some initiatives undertaken by a North American financial-services company as part of its cybersecurity plan.

In the next normal, cybersecurity will be embedded into new processes and technologies as a strategic imperative rather than as an afterthought. It is therefore more important than ever that cybersecurity leaders understand the ongoing changes in how their business is creating value. With such understanding, these leaders can dynamically modify priorities to reflect new business requirements, opportunities, and constraints.

Exhibit 2

The cybersecurity plan of a North American financial-services company focused on prioritized security opportunities in the postpandemic business environment.

Elements			
	<p>Opportunity How have the business aspirations and priorities changed?</p>	<p>Parameters What is needed, reasonable, and within funding levels?</p>	<p>Timing How forward looking do we want to be?</p>
<p>Large North American financial-services company</p>	<p>4x growth in virtual-desktop-infrastructure capacity, which rose to 80,000 instances, from 20,000</p>	<p>10% of vendors identified as critical in COVID-19 environment; for those vendors, a focused cyberresilience program was launched</p>	<p>90 days needed to automate prioritized controls</p>

The COVID-19 pandemic has changed consumer and business behavior in dramatic ways. Cybersecurity teams have generally performed far above expectations in fulfilling a dual mission of addressing new risks and anticipating the next normal. As they continue to enable changing business priorities while ensuring an appropriate

level of control, the cybersecurity teams—no longer “requirements recipients”—will become full partners with business, risk, and IT stakeholders. In the next normal, cybersecurity leaders will not only protect their organizations at scale but also make security, once and for all, an integral part of delivering business value.

Venky Anant is a partner in McKinsey’s Silicon Valley office; **Soumya Banerjee** is a cyber-solutions expert in the New York office, where **Kathleen Li** is a cyber-solutions analyst; and **Jim Boehm** is a partner in the Washington, DC, office.

Copyright © 2020 McKinsey & Company. All rights reserved.