Bolstering Cybersecurity Capabilities during Covid-19 and Beyond

The pandemic created more remote workers—and more attackers who seek to take advantage of that.

By Syed Ali and Frank Ford

BAIN & COMPANY

Syed Ali is an expert partner and Frank Ford is a partner with Bain's Enterprise Technology practice. Syed is based in Houston and Frank is based in London.

At a Glance

- Even before Covid-19, few organizations had the robust cybersecurity capabilities to combat rising attacks. The pandemic has increased the risk because of the rapid shift in work patterns and operating models.
- Hostile actors have taken advantage of the pandemic to ramp up their attacks, targeting the vast numbers of employees working from home and operations conducted remotely.
- Organizations need to take short-term actions that improve the resilience of working from home and other remote collaboration and operations.
- After the pandemic ends, companies will make remote models permanent for some employees. Managing risk for this transformation requires improvements across a full spectrum of 20 cybersecurity capabilities, with periodic reassessments.

Even before the Covid-19 pandemic, few organizations had mature cybersecurity capabilities that could meet the mounting challenges posed by attackers. Research by Bain & Company in the fourth quarter of 2019 found that executives at many companies overestimate the effectiveness of their cybersecurity and lack the strategic capabilities essential for a robust posture (see the Bain Brief "Most Companies Overestimate Their Cybersecurity, but Resilience is Possible"). We discovered that only one in four companies followed the most important cybersecurity best practices. Accordingly, it was no surprise that the number of breached records in the first quarter of 2020 hit an all-time high of 8.4 billion, a 273% surge from the same period in 2019, according to Atlas VPN.

Since the onset of the pandemic in late February, more than 40% of large enterprises have made moderate to significant reductions in IT budgets, and about 20% were cutting security spending. At the same time, around 70% of the companies we surveyed rolled out work-from-home (WFH) capabilities. These include increasing network connectivity to allow more people to connect simultaneously, shifting select workloads to the cloud to make access easier and faster, adopting new collaboration and productivity solutions like Zoom and Slack, and deploying devices like laptops along with peripherals. Unfortunately, these steps had to be taken quickly, often with rudimentary security, as companies scrambled to keep their workers productive.

The combination of these three factors—executive overconfidence in their company's cybersecurity posture, shrinking IT and security budgets, and rapidly implemented WFH capabilities—creates the conditions for a perfect storm of successful cyberattacks.

Facing increased risks

From the onset of the pandemic, malicious entities have been launching attacks with a greater frequency and intensity on remote employees and other corporate assets. Security teams have seen more attempts at intellectual property theft, particularly since late January 2020. APT41, a prominent cyberthreat group reportedly targeted companies across industries in the US, UK, Canada and parts of the European Union and Middle East using recently disclosed vulnerabilities in major vendor systems. This was one of the broadest campaigns in recent years, and its aim was long-term espionage and surveillance.

Palo Alto Networks reported a 569% increase in malicious domain-name registrations related to Covid-19 in February and March 2020, and at the end of March found more than 116,000 Covid-related newly registered domain names, of which 35% were either malicious or high-risk.

Customer information, intellectual property, sensitive communications and other data are generated, manipulated and often even stored remotely. Workers are productive, but WFH models have inherent weaknesses that will always entice attackers.

Today, at-home workers across industries perform a full set of business functions that generate large volumes of rich corporate data. Customer information, intellectual property, sensitive communications and other data are generated, manipulated and often even stored remotely. Workers are productive, but WFH models have inherent weaknesses that will always entice attackers.

Insiders have always been one of the biggest pain points in cybersecurity, and the widely adopted WFH models only exacerbate this threat. According to a 2019 report by Bitdefender, 7 out of 10 breaches over the past five years were caused by insiders, intentionally or unintentionally. Remote workers today actively seek information about the pandemic, schools, restaurants and the economy. They're more digitally connected than before the pandemic. Attackers have taken note and are using a variety of techniques to ensnare the unsuspecting individual. Remote workers put their companies at risk when they click on a malicious link, respond to a seemingly normal email request that's actually well-crafted social engineering, or download a seemingly innocuous app or browser attachment.

Devices used for remote work are susceptible to compromise due to vulnerabilities in their hardware firmware, drivers or installed applications. This applies to company-owned devices, but is especially true for employee-owned laptops that are multi-purpose and often used by other household members.

Peripherals like Bluetooth speakers, keyboards and video cameras are used by remote employees to make their jobs easier. Unfortunately, many products from trusted brands have been sold out for months, prompting companies and consumers to buy less reliable products that may be poorly supported and come with vulnerabilities in their firmware, drivers or supporting applications.

Home and public networks, along with the underlying networking equipment such as routers and hot spots, are also vulnerable and frequently exploited by attackers. Home networks host growing numbers of other vulnerable devices such as laptops belonging to other family members and smart home devices. An attacker can compromise anything connected to the Internet, then carry out malicious actions on the local network and ultimately on WFH devices.

Reacting to new threats

Most companies rolled out WFH security measures by extending a few technologies to remote devices. The most common solutions are VPNs, endpoint protection and some form of advanced authentication. The first two are basic legacy security technologies. However, even when all three are consistently used, they can't fully mitigate the inherent weaknesses in WFH models. Overreliance on basic security measures is akin to protecting workers in a crowded train with basic disposable face masks and gloves instead of robust measures like full personal protective equipment and background services like regular testing.

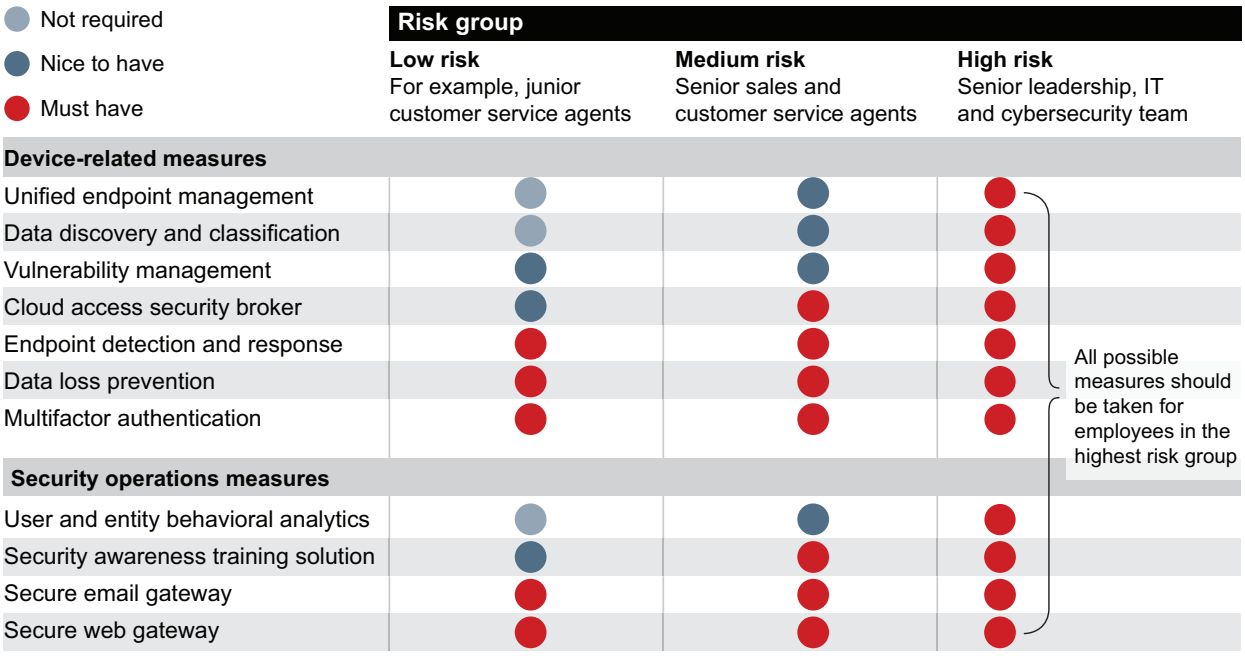
Overreliance on basic security measures is akin to protecting workers in a crowded train with basic disposable face masks and gloves instead of robust measures like full personal protective equipment and background services like regular testing.

Organizations should take two sets of actions, the first to neutralize the threats to WFH and the second to position themselves for the evolution of how work gets done after the pandemic.

First, a multidisciplinary task force is the most effective way to tackle WFH threats and improve resilience during the pandemic. The chief security officer should lead this effort, along with informed leaders with decision-making authority from parts of the business, IT, cybersecurity, as well as audit, risk, compliance functions, legal and HR.

The task force should begin by characterizing groups of remote workers and partners based on their business role and level of access. All groups should be covered by a common set of modern security technologies and processes. High-risk groups performing mission-critical functions (for example, top

Figure 1: Identifying risk levels allows security teams to set appropriate cybersecurity solutions for VPN access



Source: Bain & Company

leadership) or having the broadest or deepest system access (such as DevOps teams, system administrators and application developers) need a robust complement of security. *Figure 1* gives an example of security technologies for different users who connect using a VPN.

The task force should continue its work as situations evolve, meeting regularly to assess security measures and policies in light of the latest findings by the internal security operations (SecOps) team, industry- and company-specific threat intelligence, material changes to IT (for example, the adoption of new cloud solutions) and feedback on user experience. This involves directing activities such as:

Governance and organization

- Securing new business and technology initiatives related to the pandemic, such as process automation and redesigning supply chains to increase flexibility.
- Refining general and population-specific security-awareness training based on trends in user behavior.
- Increasing SecOps capacity to accommodate potential Covid-19 sick leave for analysts and teams.
- Establishing policy guidelines with HR, legal and privacy teams if contact tracing and surveillance are mandated for health and travel reasons.

Process and technology

- Revising software and hardware technology standards, such as minimum specifications for employee-owned laptops, and lists of approved USB, HDMI and Bluetooth peripherals for remote workers.
- Updating device-ownership policies and recommended security technologies. For example, WFH employees in the medium-risk group can use their own laptops only when they use security solutions like those in Figure 1.
- Improving SecOps by using more precise indicators of attack and compromise, incorporating internal data on compliance with revised technology standards; tighter behavioral profiling of users and devices; and stricter cloud-access and data-security policies for employees, contractors and other partners, especially in connections with high-risk regions and countries.

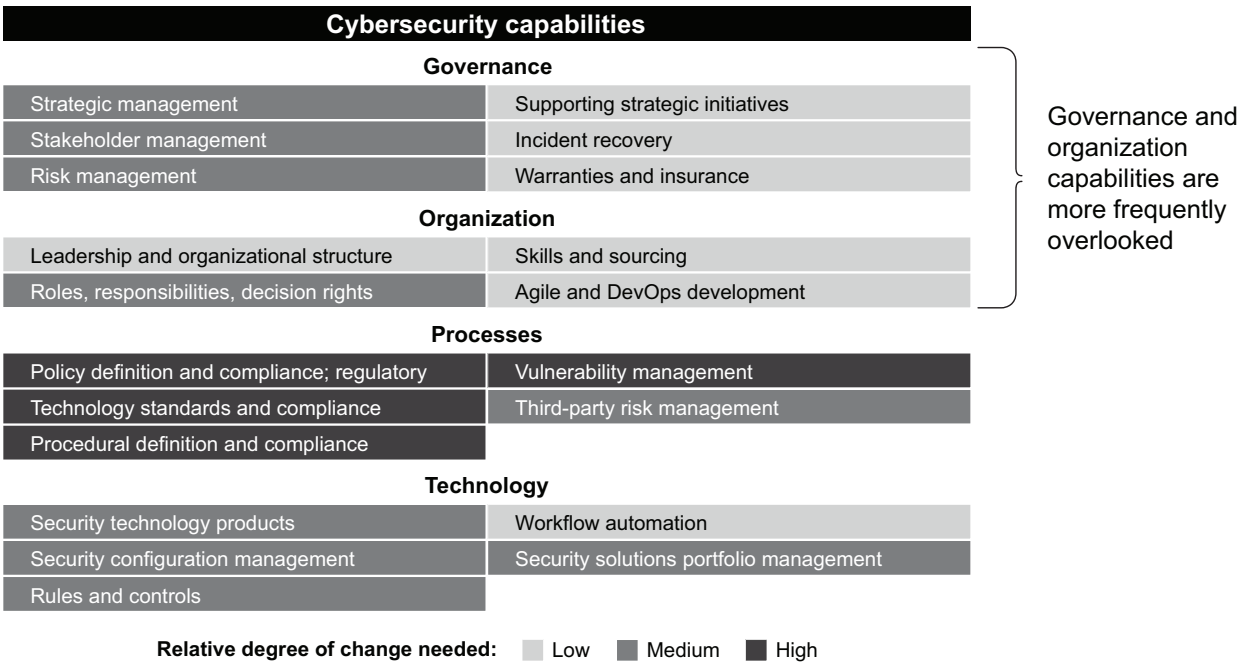
Preparing for postpandemic evolution

The second set of actions aims to strengthen a company's cybersecurity over the long term. Companies with higher levels of cybersecurity are not only adopting short-term best practices, they're designing and experimenting with next-generation technology and cybersecurity solutions. They see the current impact and future implications of working from home: employees and partners are safe, happy and productive. As we look ahead, it's becoming clear that remote work and collaboration will be a permanent part of the corporate operating model. A recent survey by HR Executive reported that 65% of workers feel they're more productive when working at home, and 20% of businesses allowing WFH are making these accommodations permanent for some of their workforce.

So while the task force helps keep the business running securely during the pandemic, the company must also reposition itself for a postpandemic world in which remote work and collaboration will be a significant part of normal operations.

So while the task force helps keep the business running securely during the pandemic, the company must also reposition itself for a postpandemic world in which remote work and collaboration will be a significant part of normal operations. That will require answering important strategic questions, such as whether to migrate from VPN to more secure architectures like virtual desktop infrastructure (VDI) or zero-trust network access (ZTNA), and whether overall cybersecurity capabilities are sufficiently robust and resilient for the new normal?

Figure 2: Among the 20 cybersecurity capabilities required for full maturity, some require more attention during and in the wake of the Covid-19 pandemic



Source: Bain & Company

To answer these questions, we recommend that companies periodically assess cybersecurity maturity in 20 areas *(see Figure 2)*. This comprehensive assessment helps executives prioritize their improvements in cybersecurity to support major corporate initiatives. While the technologies shown in Figure 1 are a subset of capabilities that help secure work-from-home operating models, thoroughly securing WFH requires improvement in each of these 20 capabilities.

In the first half of 2020, most companies reflexively secured working from home with basic technologies they were already using. This was a good start, but strong cybersecurity involves much more than implementing technology. Companies must also perform ongoing activities like adjusting technology standards and security-awareness training that help maintain a security baseline for remote work. Finally, companies have to reevaluate the full complement of security capabilities as they permanently adjust operating models for the postpandemic world.

Bold ideas. Bold teams. Extraordinary results.

Bain & Company is a global consultancy that helps the world's most ambitious change makers define the future.

Across 59 offices in 37 countries, we work alongside our clients as one team with a shared ambition to achieve extraordinary results, outperform the competition and redefine industries. We complement our tailored, integrated expertise with a vibrant ecosystem of digital innovators to deliver better, faster and more enduring outcomes. Since our founding in 1973, we have measured our success by the success of our clients. We proudly maintain the highest level of client advocacy in the industry, and our clients have outperformed the stock market 4-to-1.

For more information, visit **www.bain.com**