COVID-19: Cyber and the remote workforce

How cyber vulnerabilities and operational efficiencies are reshaping the "next normal"

What has made the COVID-19 disruption so profound is that few, if any, organizations factored a global pandemic into their business continuity planning. And, unlike the typical events around which most business continuity plans are based – cyberattacks, natural disasters, supply chain disruptions, etc. – there will not be a clean ending to the COVID-19 crisis, where everything returns to normal. COVID-19 is already causing profound and permanent changes in strategies around people, processes and technologies, and what it means to be a highly resilient organization. Simply put, the day when everyone needs to be able to work from anywhere is upon us.

The Next Normal

Almost overnight, enterprises worldwide found themselves in shut-down situations where workers had to shelter and work from home. This has created cybersecurity stressors across multiple dimensions, including:

- **“Bring Your Own Device” Explosion** – Many workers do not have company-issued laptops for home use. This means they are accessing corporate networks and systems on devices that may have vulnerabilities or are already being compromised. Likewise, workers are relying heavily on web conferencing and collaboration tools to do their jobs, which can be compromised by threat actors (the recent headlines around “Zoom-bombing” being the most prominent, but not the only example). All of this has significantly increased security complexity due to the overnight expansion of the typical enterprise attack surface.
Without IT’s knowledge, 1,000+ insecure personal devices connect to enterprise networks every day in 30% of U.S., U.K., and German companies.

- **The home computing environment** – Enterprises have no control over their workers’ home computing environment. The problems emerging from these environments during the COVID-19 crisis range from younger employees expressing difficulty working out of small apartments with roommates who are also working, to workers whose bandwidth is insufficient to deliver acceptable performance for videoconferencing. And, since everything from televisions to toasters might be connected to the internet, the typical home environment is especially ripe for Internet of Things (IoT) vulnerabilities. For a true “work from anywhere” future, security teams – and IT in general – need to develop programs and protocols that enable remote workers to perform their jobs without introducing excessive risk or productivity compromise into the organization.

- **Secure remote access** – Most enterprises simply were not ready for a world where all workers must have secure remote access to networks and systems. For organizations relying on legacy systems, this is especially problematic because they are prone to performance, scalability and availability problems. This issue was vividly illustrated by the problems many state unemployment offices had with processing a deluge of claims, due to their use of legacy COBOL-based systems, some of which are several decades old. If workers are going to be entrusted with working from home on the devices of their choice, then they also need to understand proper security hygiene and corporate security policies. And, security teams need to adopt a zero-trust model where they implement strong identity and access management, and can readily detect and respond to anomalous behavior.

- **The insider threat** – Work and economic climates will continue to contribute to an increased volume of insider threats. Leadership should consider how the enterprise is equipped to pursue a risk-based insider threat monitoring program. Knowingly or unknowingly, the majority of cyber incidents are caused by an employee of the impacted organization.

- **Insecure "ad hoc" processes** – Business processes that were designed for a secure office environment are now being executed across distributed and potentially insecure home environments. For example, before COVID-19, no bank would ever have mortgage processors approving loans out of their houses. But under the “next normal” in which we now live, banks have no choice but to adapt to this new ad hoc process (unless they stop lending all together). Near term, this means security teams must scramble to embed security and compliance into this new process, which is not trivial: they need to authenticate identities, ensure secure access of supporting documentation and link back to government systems, all from a device not issued by the company. There is no playbook for doing this, because it’s never been done before.

Moving forward, enterprises of all types will need to evaluate their in-office processes and take the steps required to enable a secure migration to a remote working environment.

Enterprises are now preparing for the post-COVID world where remote employee enablement and productivity are regular and integral to their plans. As organizations consider how to institutionalize some of the processes and functions they quickly put into place in the early months of 2020, cyber security should be a prominent player in all efforts. When done properly, with the intention of enabling productivity while securing what matters most to an organization, cyber is embedded into strategic executive discussions and into design through implementation, so the “next normal” does not become the next source of cyber risk.

COVID-19 Recovery will be the “Next Normal”

Recovery from the COVID-19 crisis will not be a clean “flipping of the switch.” Instead, it will be a phased process of people returning to work and “normal” life from specific populations, geographies (even within the same country), age groups, business segments, etc. Countries will take different approaches to getting everyone back to work, back to their economies. Since this recovery will be a first-ever undertaking, there will be mistakes, and there likely will also be infection relapses that cause the reinstitution of stay-at-home ordinances (we’ve already seen this happen with some Asian countries, and undoubtedly will see it elsewhere in the coming months).

In this environment, there is no single “next normal.” Rather, there will be a series of “next normals.” The state of society will constantly modulate until the time when there is global availability of a vaccine, which as of April 2020, healthcare professionals predict is at least one year away. It will be incumbent on cybersecurity organizations to adopt new levels of agility to adapt to this modulating environment, which raises considerable challenges.
Thriving in the future

Before the COVID-19 outbreak, enterprises devoted most of their technology and security spending on revenue generation and operational efficiency. This stands to reason, since those are generally the top priorities of an organization. The post-COVID world, however, may see a rebalancing of resources toward enterprise resilience focused on security for greater remote work capabilities in the future.

Organizations can:

1. Ensure IT teams develop and implement corporate security policies and guidelines for Bring Your Own Device (BYOD) and require that corporate security software is installed on employee devices before such devices can be used to connect.
2. Review and establish corporate firewall rules for remote access, User and Entity Behavior Analytics (UEBA), and file integrity monitoring, to effectively implement for remote employees.
3. Restrict unapproved personal devices from your corporate network and limit personal device access to only required corporate cloud services that are needed for critical business operations.

This will drive renewed interest in technologies that enable secure remote access and productivity, including:

Virtual desktop infrastructure (VDI) and desktop as a service (DaaS). These will mitigate the issues around people using unapproved devices to access enterprise computing assets by enabling security and IT teams to centrally manage user desktops, giving them far greater control than is possible with traditional desktops. VDI has been around since the early 2000s, but was slow to take hold due to complexity and performance issues. Today, however, with cloud-based VDI and desktop-as-a-service offerings, those issues have been largely mitigated, making VDI a powerful solution for the work-from-anywhere future.

Identity and access management (IAM) has also had adoption issues resulting from cost and complexity. Like VDI, the emergence of cloud-based IAM solutions has dramatically reduced the technical complexity, making it practical for security teams to implement enterprise-wide deployments. Organizations can also look to identity providers to enable and manage this capability, in many cases, with greater output of the solution and lower overall cost to the organization. IAM is central to adopting a zero-trust architecture, which will be required by most organizations seeking to appropriately manage risk with a large-scale remote workforce.

Cloud migration stands to gain greater velocity as a result of the COVID-19 pandemic. Enterprises relying on legacy systems are experiencing woeful performance, scalability and availability issues with their on-premise infrastructure. This will accelerate the migration of these systems to the cloud, or a hybrid cloud environment, with the cyber security team as a pivotal component of the process to ensure that all the cyber considerations, benefits and risk, are being weighed and implemented.

Cloud-native organizations have fared well during the COVID-19 disruption. They already had fully embraced modern cloud, identity and remote access technologies, so moving to a 100% remote workforce model was a relatively small step. The organizations struggling the most are the ones that have put off the need to mature their cyber posture across the enterprise.

The Future of People, Process and Technology

Enterprise performance is driven by people, process and technology. All three need to be addressed to effectively execute the digital transformation required to enable a world where remote workforces are the norm versus the exception.
How and where we work will be one of the most pronounced changes of the COVID-19 pandemic, as many enterprises experience the morale, cost-saving and productivity benefits of a remote workforce. The enhanced trust this requires between employers and employees will be a positive outcome of this experience, and flexibility will become the new norm – both from employer and employee perspectives. Early feedback from around the world shows this sits quite well with younger employees, who tend to place a high value on flexibility and work-life balance. COVID-19 is actually accelerating the presence of their value system in the business mainstream.

From a cyber perspective, the cyber posture and security hygiene of organizations may naturally improve as a result of the pandemic. Core security functions like patching, vulnerability management and cyber-awareness programs are likely to be better tended to and maintained. The opportunity comes in taking lessons learned from what was needed, as well as created out of necessity, and transforming those into the next-generation of security and capabilities.