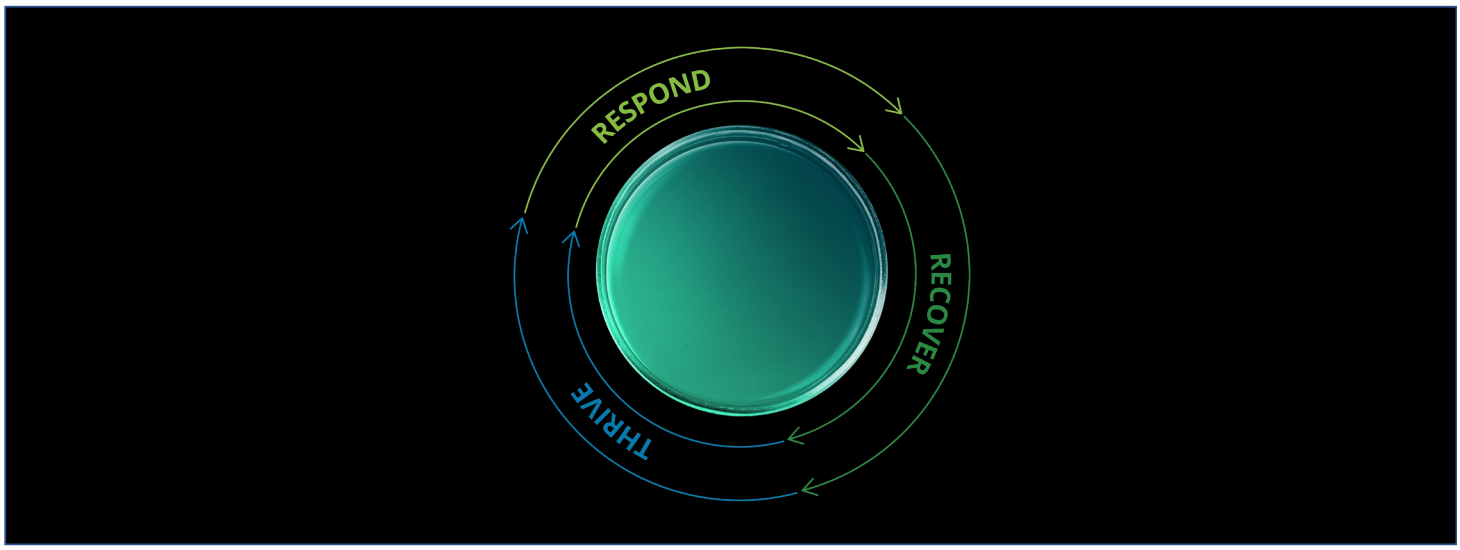
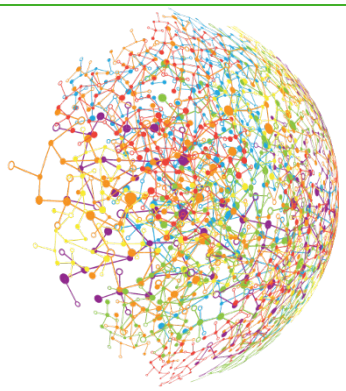
Deloitte.



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.

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.

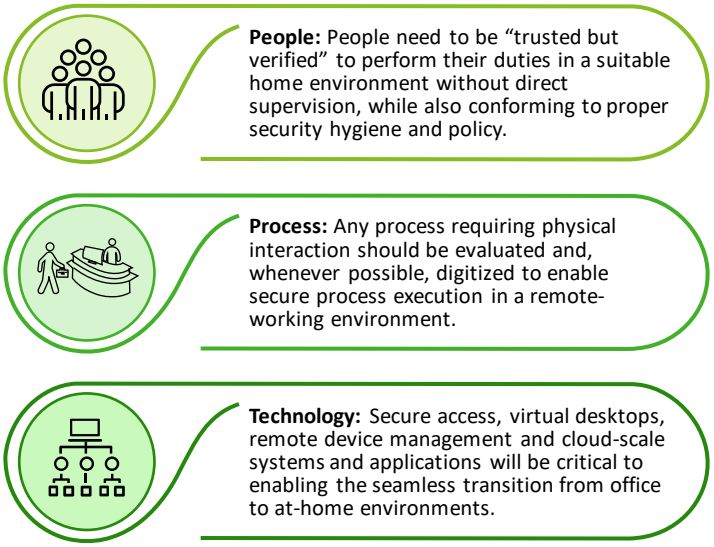
- Identity and access management (IAM) has also had adoption issues resulting from cost and complexity. Like VDI, the emergence of cloud-based IAM solutions has dramatically reduced the technical complexity, making it practical for security teams to implement enterprise-wide deployments. Organizations 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.

Contact us

Emily Mossburg
Global Cyber Leader
+1 571 766 7048
emossburg@deloitte.com

Amir Belkhelladi
Canada
+1 514 3937035
abelkhelladi@deloitte.ca

Simon Owen
North South Europe
+44 20 7303 5133
sxowen@deloitte.co.uk

Deborah Golden
US
+1 571 882 5106
debgolden@deloitte.com

James Nunn-Price
Asia Pacific
+61 293227971
jamesnunnprice@deloitte.com.au

Peter Wirnsperger
Central Europe
+49 40320804675
pwirnsperger@deloitte.de

Nicola Esposito
Spain
+34 918232431
niesposito@deloitte.es

For more information contact visit Deloitte.com/covid or Deloitte.com/cyber

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/aboutto learn more about our global network of member firms.

Copyright © 2017 Deloitte Development LLC. All rights reserved.