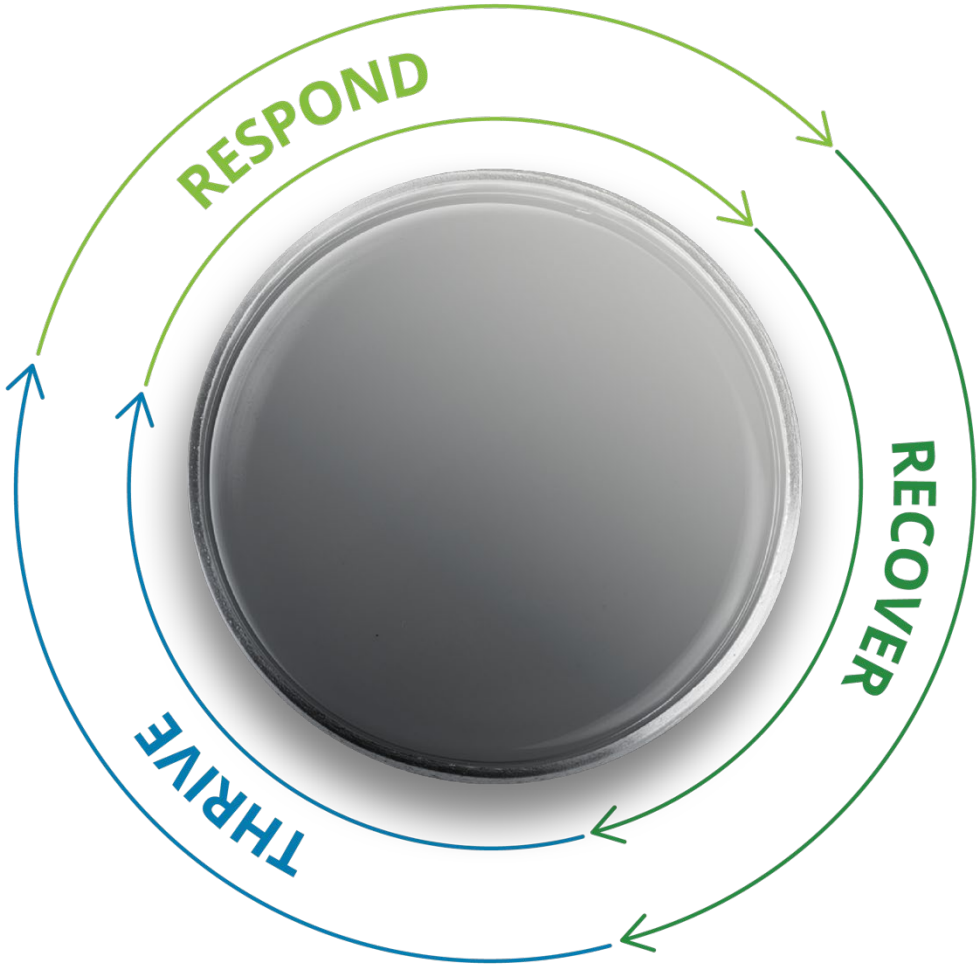
Deloitte.

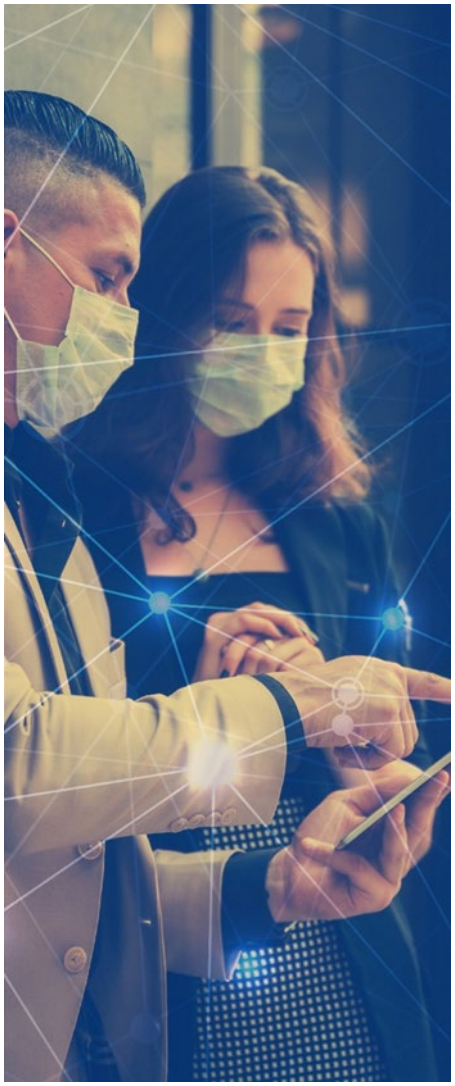


Work from anywhere. Cyber everywhere.

Work from anywhere. Cyber everywhere.

The COVID-19 pandemic forced business leaders worldwide to respond with unprecedented speed and efficiency to new ways of working, new ways of innovating, responding, collaborating, transacting…surviving. Now, as organizations begin to plan for a post-pandemic world, they must ask themselves, “how can Cyber help ensure our new ways of work are productive, sustainable, secure, and safe?”

In the first half of 2020, as companies responded to the coronavirus outbreak, they relied on Cyber to secure the networks that allowed employees to work from home and collaborate safely online together, often boosting productivity in the process. Cyber gave companies confidence to manage supply chains remotely, while also safeguarding the integrity of the processes and data shared. In some cases, Cyber enabled organizations to expand their businesses and delivery systems online in ways that many had only talked about before the crisis. COVID-19 taught us to be more flexible and patient and forced us to see new ways of doing our jobs from anywhere, at any time. Tools such as Cloud computing made that flexibility possible. But moving significant components of a business to the Cloud also required protecting systems against the threats that this new flexibility created.



Cyber became the conduit to capability and connection. As COVID-19 spread from person-to-person, country to country, and beyond, Cyber delivered the integrity and availability of the networks needed to "work from anywhere" and the confidentiality to transact and transform with confidence across geographies.

For the world to continue to thrive in this new remote, virtual environment, even as COVID-19 wanes and surges in various regions, the fundamental principles of cybersecurity are more important than ever:

- Confidentiality – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [i]
- Integrity – Guarding against improper information modification or destruction including data integrity, ensuring data has not been altered in an unauthorized manner, and system integrity, ensuring the quality that a system has when it performs its intended function in an unimpaired manner.
- Availability – Ensuring timely and reliable access to and use of information.

Adhering to these principles in the wake of a global pandemic can be challenging. For organizations to deliver on these principles and navigate the pandemic pitfalls ahead they will need to: establish a foundation of trust, adopt a "Cyber Everywhere" mindset, embrace a culture of perpetual resilience and lead from the front.

Establish a foundation of trust

Adherence to those core security principles can help provide trust between an organization – it's employees, customers, vendors and beyond. Trust affects all stakeholders, and the COVID-19 pandemic has underscored the need to reassure both customers and employees of an organization's trustworthiness. Organizations that created new workforce strategies and customer service approaches under pressure during COVID-19 will need to determine if they warrant longer term adoption and transform the ad hoc procedures into best practices for moving forward. There are four types of trust: physical, emotional, financial, and digital. From a Cyber lens, digital trust is a critical facet of our ability to thrive in the next normal, and that is not just an operational expression but a relationship challenge.

It is increasingly important to understand your specific stakeholders and their unique concerns. While Cyber can help to transform the physical workspace into new virtual environments, it can also bring to light new concerns around safety and privacy. Customers, vendors and supply chain partners want to know that cybersecurity is a priority for the organizations and institutions in which they are entrusting their transactions, information, and personal data. Employees want to feel certain that their work-related data is secure, and that the networks they need to do their jobs will function properly. Organizations should anticipate these needs and ask themselves what they must do to build and maintain trust.

Digital trust: Can stakeholders trust that their information is secure?

- ***How will we create safe, trusted virtual environments?*** Guide and monitor how teams are collaborating remotely, ensure employees are notified and aware of the approved collaboration tools and associated processes. Enforce the use of multi-factor authentication for remote access technologies (e.g. VPN) and email services (e.g. Office 365).
- ***With more data, more connectivity, more access, do we understand our cyber risk and are we confident our Cyber program will maintain and strengthen trust?*** Finding and knowing where the most vulnerable areas are within an infrastructure and systems is an important first step in building a top-tier cyber program. Use this knowledge to minimize weaknesses and enable a robust digital environment that is highly reliable, available and secure.
- ***Are we proactively detecting for fraudulent activity and cybercrime?*** Ensure that financial transactions are secure, and systems operate with integrity. Monitor the dark web to identify organizational exposures and historical, active and planned attacks against your organization. Perform sentiment analysis to improve COVID-19 staff, supplier and customer communications.
- ***Is data collected ethically and protected appropriately?*** Embed Cyber and data governance into systems that enhance safety measures in the physical space. Educate personnel involved in data collection about their new responsibilities as data collectors and stewards of security and privacy.

With the right focus, governance and funding, data security and privacy can drive business differentiation and build stakeholder trust. It will be critical for leaders to instill trust that personal data is being properly handled and safeguarded. Striking the right balance between secure transactions, data privacy and positive user experiences is crucial for organizations to confidently expand online services and customer reach. By getting this human dimension of technology, security and trust right, leaders can drive sustainable success for their organizations. Intentionality about trust during a time of crisis can set apart a business leader or organization who competently steers his or her company through these uncertain times.

A trusted leader is most often a *resilient* leader.[ii]

Adopt a Cyber Everywhere mindset

Many organizations already have determined they will never return to “business as usual” or “business before COVID” because they’ve seen increased productivity from a more virtual workplace and they want to lock in those benefits. But to thrive in this next normal, organizations need a sound strategy for managing cyber risk. A “Cyber Everywhere” mindset is required. It means understanding the pervasiveness of Cyber and meaningfully embedding it in innovation, strategy, and process to ensure that Cyber enables the success of every initiative, allowing organizations to move more quickly, effectively and securely.

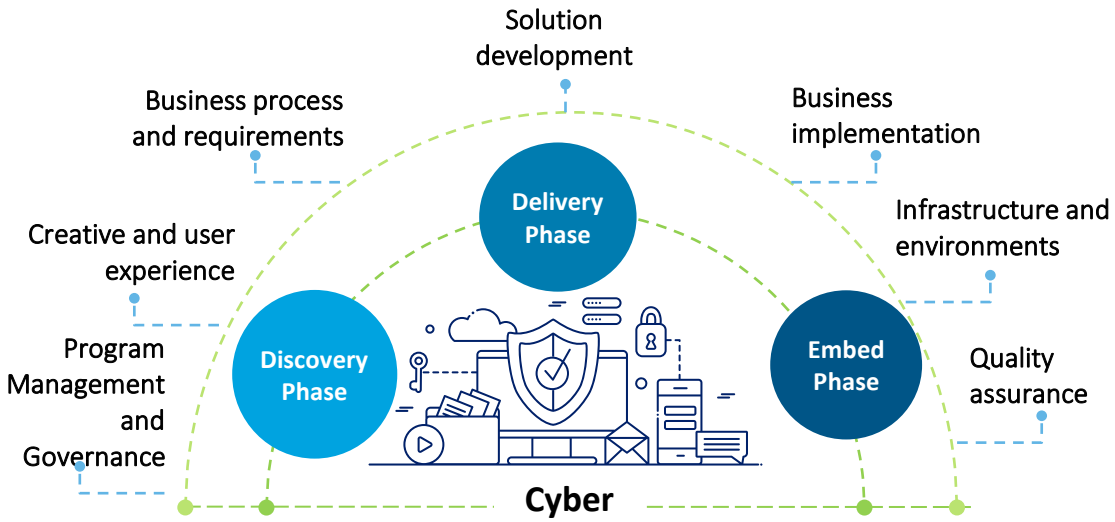
When countries and economies ordered employees to shelter-in-place, organizations quickly ramped up remote work environments enabled by extended technologies like Cloud, which hopefully meant also beefing up security around them. As organizations now shift from temporary working scenarios to sustaining a “work from anywhere” construct, companies need to reevaluate the newly expanded cyber-attack surface caused by thousands of new devices and locations now part of their environment.

Temporary will need to give way to more permanent adoption of the necessary and required collaboration and productivity tools enabled by Cyber, such as identity and access controls and privacy and data protection solutions. Data protection and security requirements around personal equipment that work-from-home employees may have pressed into service during the pandemic will need to be incorporated into Cyber programs. By considering "cyber first" in new workforce strategies, organizational leaders can unlock business value of a flexible workforce while maintaining the security and integrity of their most valuable asset.

Historically, when organizations introduce new products, new ways of working, or new operational constructs, they focus on the functional and technical requirements, often leaving the security impact and requirements of those new initiatives until later. Doing so, often slows the release of new products or causes recalls in new technologies. This situation has been exacerbated by the spike in demand for just-in-time solutions brought about by the pandemic.

We have an opportunity to leverage this time of intense innovation to increase potential for long-term success in work[iii1]. In adopting a "Cyber Everywhere" mindset, new products and new ways of working embed cyber functional and technical requirements across the lifecycles of innovation and development to make confidentiality, integrity, and availability an integral part of those initiatives – bringing the fundamental cyber principles to the forefront of new capabilities, streamlining design or delivery.

Cyber connects and enables phases of product and software development to embed confidentiality, integrity, and availability at the core



Organizations face mounting pressure to digitize and innovate quickly so they can keep ahead of competition, increase operational efficiencies, improve customer experience, and employ enhanced analytics to make better business decisions.

By including the Cyber team early during the requirements and development stage for new technologies needed, the Cyber organization can support innovation and operations to understand potential cyber risks and define security and privacy requirements, including user security profiles, segregation of duties and workflow rules. A secure concept approach can increase outcomes and efficiencies.

Embrace a culture of perpetual resilience

During COVID-19, we've seen an exponential increase of cyber threats such as ransomware and phishing schemes deployed on organizations and government agencies, from healthcare organizations to business productivity applications, across the globe. We have established that Cyber is everywhere and so is the need for organizations to adopt a culture of perpetual resilience. In order to have it, they will need an incident response program, a culture of cyber awareness and that is well understood, and a strong foundation of good cyber hygiene.

In this next normal, the ways we live, work, transact, and communicate will be even more interconnected. The concept of "superjobs" and "superteams" will integrate AI into teams, combining people and machines to leverage complementary capabilities to solve problems and fundamentally transform the way we work[iv]. A weakness anywhere in the chain could affect the entire network and undermine the ability to work confidently and competently. A laptop with a vulnerability – or any point of interaction with technology — can bring down an entire system that was intended to be flexible and efficient.

Like the coronavirus itself, cyber threats have spread quickly over the past few months, often without recognizable patterns and sometimes without a perceived or even an intended target, unleashing havoc at random on industries and individuals who were experiencing their own levels of chaos and transition. Containment of these cyber incidents can mean cutting off systems and shutting down operations to stop the spread, often leaving organizations debilitated not just for days but for weeks or longer, leaving their organization vulnerable to financial and reputational harm, and individuals reeling with lost identities, stolen stimulus payments, and eroded trust.

Companies need to build resilient cyber capabilities to rebound stronger and adapt more quickly to new global crises and cyber threats without losing critical operational function and customer confidence. Thwarting these attacks takes an intentional approach to creating and cultivating a cyber aware culture. It's not just about good decisions from the top, employees at all levels of an organization should understand the importance of and their role in Cyber; everyone should learn how to spot, report, and respond to cyber threats.

> If an employee can't reach the tools needed to do their jobs, then productivity will be impacted and ultimately go down. Employees access to systems requires them to be available; for them to up and working.

It's incumbent upon organizations and government institutions to reevaluate their incident readiness and response capabilities considering evolving and expanding attack surfaces, new connections, and increasing number of endpoints. Overall attention to cyber hygiene will enable them to adapt and pivot to new challenges and opportunities.

In evaluating the organization's incident response posture, executives should ask these simple questions:

Questions to ask about incident readiness and response

- Do you have a plan for effectively managing a cyber incident when it hits you, your suppliers, vendors or other organizations you work with?
- Do you feel sufficiently informed to pre-empt cyber-attacks and make investment decisions both strategically and in response to an incident?
- Do you feel confident that you have done all you could to proactively mitigate the potential impact of a cyber-attack? Could you evidence this to your board or regulators?

Cyber hygiene is the foundation of perpetual resilience

Good cyber hygiene isn't much different than good dental hygiene. If you brush and floss your teeth twice a day, you are less likely to experience painful dental incidents, such as a root canal. If an organization puts in place preventative security measures and fastidiously tends to them, then the likelihood of a catastrophic cyber event is minimized. Good cyber hygiene is essential for organizations to adapt and thrive and should not be reduced or ignored in the wake of shrinking budgets due to the pandemic.

A keen eye on cyber hygiene across the enterprise will help maintain a protected digital environment and reduce overall cyber risk for the organization. Operational processes, remote connectivity requirements and security, remote connection volume, and user awareness must be reviewed to identify and prioritize the risks associated with an expanded virtual workforce.

Tenants of good cyber hygiene: protect all company critical and sensitive information from theft or loss

Security Policies
Update and remind all employees of security policies

Availability
Ensure adequate capacity for remote connections to perform critical roles

Vulnerability Management
Install software updates regularly to ensure patches are up to date

Access Management
Ensure authorized devices and protocols are used for remote

The benefit of good cyber hygiene is that organizations start to create an environment where the secure thing to do, is the easy thing to do. Cyber hygiene is the foundation of perpetual resilience that will enable organizations to thrive in the future.

So, what do organizations need to thrive in the next normal? Here are ten components of an effective Cyber program:

10 components of successful Cyber programs

Culture awareness and training:

- Establish and implement heightened employee security awareness, education & training in accordance with increased threats from COVID-19; leverage SOC analysis to create an agile, data-driven security awareness strategy.
- Engage with human resources to make security a fundamental part of every employee's job requirement.
- Reevaluate the cyber organization and operating model to ensure the best talent is allocated to critical roles and devise a plan to cross train resources or employ digital FTEs to close skills gap.
- Engage in the concept of Cyber "superteams" and augment existing workforce with AI to collaborate and create more workforce capacity to execute on strategic Cyber goals.

Data and privacy:

- Ensure balance between right to health and right to privacy. Consider confidential IP, PII and PHI data consumption and transfer monitored during COVID-19 and in the 'next normal'.
- Limit the collection, use and disclosure of personal information to what is necessary to prevent and manage COVID-19, and take reasonable steps to keep personal information secure.
- Define a process to examine if your aggregated data contains confidential or restricted information before sharing for any purpose.

Incident response:

- Update required stakeholders and cyber incident response plans to reflect COVID resurgence plans, remote workforce, and organizational and customer impact.
- Practice and test incident response plans through cyber wargaming and tabletop exercises with those stakeholders.
- Ensure that alternate communication channels are identified and established for all internal/ external communication.
- Review guidelines from security agencies (e.g. NIST) and ensure that appropriate actions are incorporated in the incident response plan.

Identity and access management:

- Secure identity access to provide a more seamless experience for workforce, third parties, and customers.
- As the shift to remote work continues, organizations will also need to adopt a security-first cloud strategy to strengthen privilege access management.
- Enforce MFA or step-up authentication based on the access requests
- Proactively monitor privileged identities.

Security governance:

- Review and update security governance models, operating procedures and security strategies to include new workforce models and cyber constraints.

Security architecture:

- Provide technology support for rapid design and deployment of systems, support IT with secure design.
- Expand and update security architecture to include additional use cases related to COVID 19 (e.g., Virtual healthcare delivery and insider threat).

Security operations:

- Harden existing security operations to match the current threat landscape.
- Establish certified incident investigators, systems availability management, and security system operations management.
- Take proactive measures to reduce the attack surfaces in a remote working model.

Technical resilience:

- Don't let back-ups be your un-doing. Prioritize business-critical processes to recover and map business critical processes to supporting infrastructure.
- Traditional recovery tends to result in aggressive data redundancy for critical systems. When malware is introduced, this backup environment can accelerate the spread of an attack. To address this issue, set up a storage vault to house backup data and other critical materials and a streamlined data recovery zone that allows you to reconstruct your environments from the vault.

Threat monitoring and detection:

- Integrate threat intelligence with security event monitoring and activate vulnerability detection and threat hunting make use of the most recently updated monitoring dashboard designed for COVID-19.
- Engage in communications with employees and third parties/ supply chains to reduce vulnerabilities.
- Implement automation platforms to improve and automate monitoring, investigation and triage of security incidents.

Third party risk management:

- Perform third-party security reviews to identify vulnerabilities.
- Review vendor risk management frameworks, third party risk management operating models, planning, control implementation and monitoring procedures
- Evaluate Managed Security Services providers in terms of efficiency and effectiveness
- Monitor & evaluate third party resilience throughout the period of disruption

Leading from the front

The coronavirus crisis just may be the catalyst for transforming the cyber security function, propelling it to a position of greater prominence and strategic importance within organizations. No longer relegated to the Chief Information Security Officer (CISO) only, all senior leaders and board members must take responsibility for cyber risk in the enterprise. As our workforce transforms in the wake of COVID-19, so does our fundamental understanding of how Cyber can enable and propel us forward.

Leaders of organizations public and private, big and small, should understand the critical role that Cyber will play in creating stability and laying the foundation for their companies, customers and citizens to thrive in the post-pandemic economy. Organizations that properly integrate Cyber now will be able to better ensure confidentiality, integrity and availability, the core principles of security, as they adapt to survive and thrive.

That understanding comes with the opportunity to lead the cultural transformation that embraces Cyber as a strategic enabler to achieving an organization’s mission. Executives across the enterprise can demonstrate their visionary leadership by helping to guide and shape strategy with Cyber embedded in the conversations and outcomes. It should go without saying that executives understand their organization's risk profile and can provide knowledge of where vulnerabilities may exist within their systems. This knowledge allows them to make executive level decisions on whether to accept or how to best mitigate cyber risks. Having leaders embrace the risk conversation and commit it to their daily dialogue will only benefit the outcomes of these efforts.

Concurrently, CISOs can no longer be viewed as simply compliance monitors and security enforcers. Today’s CISOs should be connected to and collaborating more effectively with the business to manage cyber risks, and work toward that culture of shared cyber risk ownership across the enterprise. This has already been recognized as a need by CISOs but the impact of COVID-19 on organizations has created a symphonic opportunity that reinforces a new kind of leadership that prepares for such disruption, again and potentially again. COVID-19, for all its challenges, has also given us the opportunity to remold the new tomorrow.

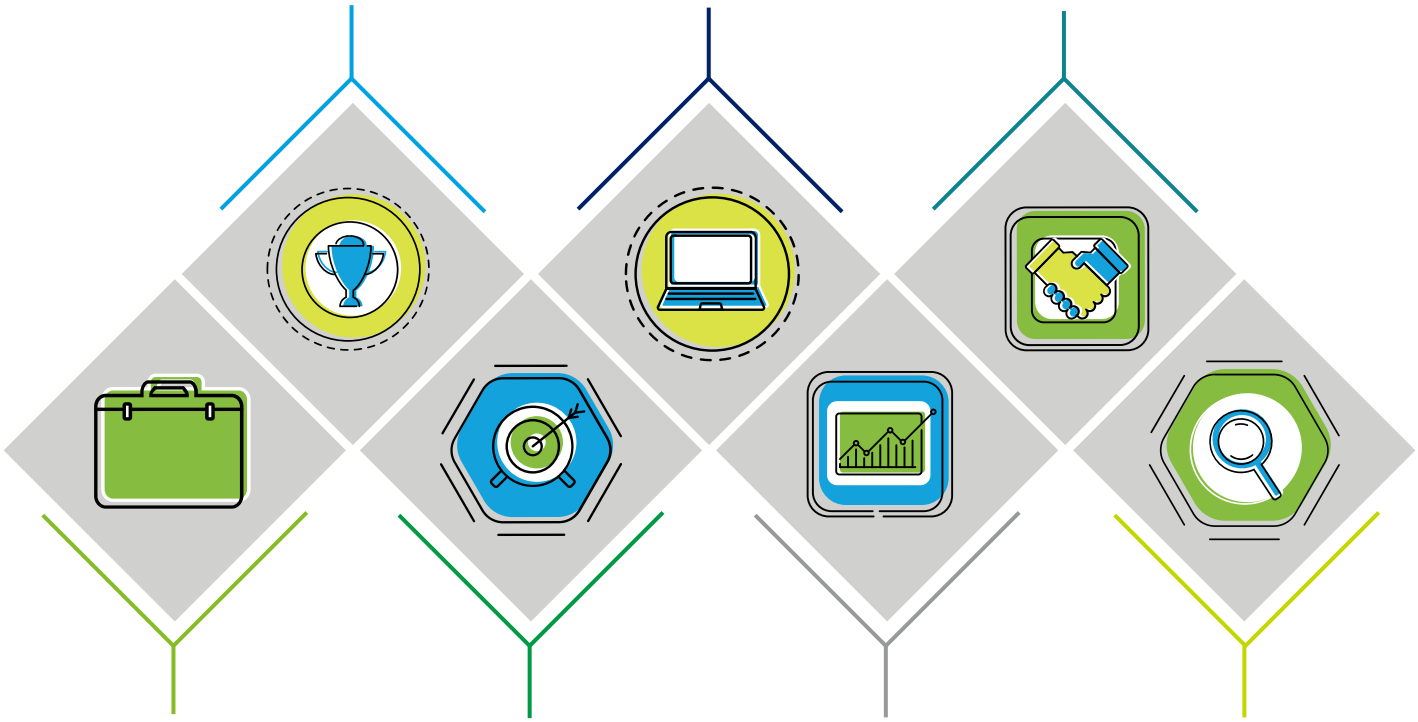
We will lean on Cyber more than we have ever before from education to customer interaction and transactions, from securing the supply chain to assessing cyber risk in a merger and acquisition (M&A). The responsible, resilient leaders of the future will begin to ask themselves a revised set of questions to help them thrive in that new tomorrow.

7 Questions every executive should ask about their Cyber posture to thrive in the next normal

Do our business leaders understand what the organization's most valuable assets are and the level of cyber risk they are accepting?

How do we secure our services and offerings for the next normal where all my customer interactions are digital?

How should we reset our global supply chain footprint to improve resiliency?



Have enterprise roles and responsibilities related to cybersecurity been clearly defined and communicated at every level of the organization up to the CEO and the board?

Are technology solutions designed, integrated, and operated with security and privacy in mind?

Does the business incentivize the adoption of cyber assessment and practices on the businesses and products in which it invests?

Are third-party (and beyond) risks managed with a cyber-risk lens in order to mitigate cyber impact directly or indirectly created from supply relationships?

Cyber everywhere. Succeed anywhere.

Cyber is everywhere, and if left unattended it could prohibit organizations from successfully navigating the road beyond the pandemic or it could be the mechanism that will enable businesses to respond effectively to future threats, to remain flexible, adapt to sudden changes in the market, and live to thrive again.

As organizations move from the recovery phase and prepare to thrive in the new COVID-transition era, Cyber has become the conduit by which they can transform their businesses and prepare for the next set of normals. Cyber is enabling new ways of delivering services, new methods for selling products, and new approaches to interacting with customers. It continues to help organizations deliver upon those key security principles of confidentiality, availability and integrity to enable workforce transformation, secure transactions and interactions. Done right, Cyber can help safeguard the data integrity and utility of new contact tracing applications. And, of course, securing infrastructure of systems will help support the networks that permit employees to continue to work from anywhere, either by choice or to ensure social distancing guidelines in the workplace.

Effective cyber risk management can help businesses achieve smarter, faster transformation and stay ahead of the threats during these uncertain times as well as help organizations achieve the ultimate goal —building trust and resilience among their customers, employees, governments and communities both now and into the future.

Authors

Emily Mossburg

Global Cyber Leader | Global Risk Advisory
US
+1.571.766.7048
emossburg@deloitte.com

Amir Belkhelladi

Canadian Cyber Leader |Risk Advisory Canada
+1514.393.7035
abelkhelladi@deloitte.ca

Nick Galletto

Future of Work | Risk Advisory Canada
+416.601.6734
ngalletto@deloitte.ca

Jeff Schwartz

Workforce Transformation| Deloitte Consulting
US
+1.212.653.2532
jeffschwartz@deloitte.com

Tina Witney

Workforce Transformation | Deloitte Consulting
US
+1.973.602.5029
twitney@deloitte.com

Jonathan Pearce

Talent Mobility | Deloitte Consulting
US
+1 646.301.1407
jrpearce@deloitte.com

Contributors:

Tara Mahoutchian, Senior Manager, Human Capital
Nicole Hockin, Senior Manager, Global Risk Advisory | Cyber

Deloitte.

[i] CNSSI 4009, Committee on National Security Systems (CNSS) Glossary, dated April 6, 2015. NIST SP 800-12 REV. 1 AN INTRODUCTION TO INFORMATION SECURITY 3
[ii] Deloitte Insights, Embedding Trust in Covid-19 Recovery, April 23, 2020
[iii] The social enterprise at work: Paradox as a path forward. 2020 Deloitte Global Human Capital Trends
[iv] The social enterprise at work: Paradox as a path forward. 2020 Deloitte Global Human Capital Trends