Orchestrating a resilient digital risk program

Augment your digital risk resilience during a crisis

The COVID-19 crisis is disrupting and changing the technology risk and security landscape. The role of digital risk leaders—including CIO, CRO, CSO and CISO—in fortifying risk & security while acting as a business enabler is critical.

We understand what you are facing

During the current health crisis, organizations of all sizes are moving into crisis mode: evaluating and prioritizing business critical imperatives, and forcing risk functions to re-evaluate their role to ensure business continuity. A risk-based approach to prioritizing security and privacy is a well understood concept; with the global pandemic, however, these approaches are being put to the test.

CISOs, CROs, CIOs, CSOs continue to focus on protecting the integrity of the business. As digital risk leaders, you are mapping out your critical processes and assets and ensuring systems are in place to protect them—all without compromising critical business functions.

Re-evaluating your risk approach

Many organizations are re-evaluating their risk-based approach to managing digital risk in order to carefully and rapidly respond to the complexity of COVID-19. This can include: immediate recovery from disruptions to core and supporting business operations; rejuvenating risk functions by implementing strategies to rollout "lean" risk practices; and addressing alternative working arrangements.

As more remote workers gain access to data, information, and network resources, expect an imminent rise of attention from bad actors. As your organization's security posture evolves, so too will your approach to managing digital risk. It is critically important to:

- **Re-evaluate your critical assets** – with changing work environments, end points and employee access, do we have an accurate picture of our critical assets and their security protocols?
- **Re-evaluate risk and reporting benchmarking** – are we reporting the right risk and benchmarking metrics given the shifting security and risk landscape of the organization?
- **Re-evaluate risk-as-a-service** – are we strategically supporting our critical functions and priority initiatives?
- **Revitalize resilient risk platforms** – are we leveraging technology sufficiently to manage risk identification, monitoring and reporting practices seamlessly across the organization?

How we can help

Our KPMG team is a cross functional group that applies risk-based concepts to provide business-focused, technology-enabled skillsets and plug and play solutions to help rapidly orchestrate a resilient digital risk program. Services include:

Out-of-band incident response platform

- Integrated incident response program across BCP/DR, Cyber, Fraud, Physical and other sources
- Deployed with out-of-band network option for minimum business disruption during crisis, breach & outage protocols in effect
- Plug & play solutions with orchestrated workflows and incident response playbooks
- Integrated risk management taxonomies for business risk context and insights.

Other digital risk services

- Digital "crown jewel" readiness exercise
- Integrated risk management re-boot (digital risk quantification and remediation)
- Risk-as-service solutions.

Key contacts

Sree Kunnath
Partner,
Technology Risk
416 791-2001
skunnath@kpmg.ca

Hartaj Nijjar
Partner,
Cyber Risk
416 228 7007
hnijjar@kpmg.ca