As COVID-19 struck suddenly across the globe last year, work-from-home became a new norm for almost every organization. Likewise, cybersecurity operations also faced tremendous new challenges. Now that businesses are slowly transitioning back to on-premises job models, a considerable percentage of employees is still expected to work from home on a rolling basis to maintain social distancing at workplaces. Cybersecurity leadership, particularly Chief Information Security Officers, are taking strategic and stronger roles within their organizations during this time of crisis that still prevails. The work structure may have turned hybrid, but there is still a large-scale adoption of work-from-home technologies and a much greater usage of cloud services than ever possibly imagined. This has made it all the more challenging for the leadership to maintain a balance and ensure the safety of their business and informational assets with onsite and offsite workforce.

**New Security Challenges in the New Normal**

COVID-19 pandemic has opened up never-faced-before challenges for security professionals such as:

* Work-from-home has allowed for multiple cyberattack vectors to exist due to increased dependency on home networks and personal devices.
* Potentially easier and more effective social engineering attacks due to a dispersed onsite and offsite workforce.
* Security Operations Centers (SOCs) that have been designed to identify irregular behaviors have limited visibility due to the new work norms.
* Public sectors such as healthcare services and hospitals have been particularly hit hard by new types of ransomware that aims at disrupting services and conducting Denial of Service Attacks.

Cybersecurity leaders now need to move beyond compliance monitors and work towards shared risk ownership within the organization. The daunting challenge for the leadership is to protect the organization’s digital assets and infrastructure while ensuring operations without interruption. For instance, cybersecurity teams are now adjusting their risk management and security programs to enable adoption of cloud services and work-from-home tools.

According to a new report by World Economic Forum titled “Cybersecurity Leadership Principles: Lessons Learnt During the COVID-19 Pandemic to Prepare for the New Normal”, there are five proposed principles to balance short-term goals with medium to long-term goals.

1. **Foster a culture of Cyber Resilience**

With the digital ecosystem being a dynamic environment, cyber threats often evolve before regulations. During the pandemic, it’s important to prioritize incident response, business continuity and recovery activities. They need to strengthen their employee’s cyber resilient behavior even more than before. Every day, as employees make decisions impacting security, keeping the organization secure is everyone’s responsibility. Security leaders need to help employees stay secure by regularly training them to identify phishing attempts, scammers, online [credit card](http://www.cardzgroup.com/BankCards.html) fauds, and proactively educating them about new techniques arising during the pandemic.

1. **Focus on Protecting the Organization’s Critical Assets and Services**

Cybersecurity leadership should have a systemic and holistic view of their critical applications, services, assets and suppliers to determine potential consequences of a crisis to their employees, revenue, customers and continuity of important services. Hence, it’s imperative to maintain strong cyber hygiene by keeping an inventory of critical digital assets to ensure a vulnerability management strategy. They must have a layered access mechanism in place to allow access of critical systems to privileged users.

For securing remote connectivity, organizations need to implement layered defense for preventing data leakage and detecting suspicious activity from remotely-connected endpoints. To decrease the time of detection till mitigation, businesses need to invest more and enhance their monitoring and response capability. Remotely monitor collaboration tools, employees and even third parties to catch abnormal behavior on time.

1. **Balance Risk-Informed Decisions During and Beyond the Crisis**

With business risk posture significantly changed, the leadership needs to balance their risk-informed decisions for post-covid times in the long run. With a high-velocity of new applications developed to cater to the changing market, many have failed to resolve configuration issues or bugs in their applications and introduced them hastily. Hackers can proactively identify and exploit weakest links in a value chain, and hence it’s imperative to adopt no-trust approach to secure supply chains.

1. **Update and practice your response and continuity plans as your business transitions**

For every business continuity program, crisis management is a key component. Organizations that focus only on analyzing and mitigating risk cannot handle sudden crisis very well. For a crisis as big as the pandemic, it’s important to build a cross-functional team with a detailed plan to orient individuals with diverse roles.

As digitalization continues to accelerate, managing cyber risk should adapt with speed and agility to align effectively with risk appetite and strategic business priorities.

1. **Strengthen Ecosystem-wide Collaboration**

Private and public-sector leadership should collaborate and ensure participation in initiatives to secure ecosystem against existing and emerging cyber threats. Moreover, businesses must also come on the same page with suppliers to implement cybersecurity controls for encouraging third-party regulatory alignment.

**The Way Forward**

Organizations cannot expect cybersecurity leadership to achieve faultless security in today’s context. However, effective management of cyber risk can help businesses achieve faster and smart transformation and stay ahead during these uncertain times. The end goal of businesses is resilience.