When the COVID-19 pandemic struck all over the world last year, remote work was suddenly the new norm. As a result, the cybersecurity industry also faced many challenges. Even though many organizations have slowly begun to transition back to onsite jobs, the work model has still not entirely shifted back to how it used to be. Till the pandemic is completely over, a large number of employees still have to work remotely in shifts in order to keep the social distancing practices in place. Leaders in the cybersecurity industry, specifically the Chief Information Security Officers, now face stronger and strategic roles in their organizations. Although the work model is now hybrid in nature, still, there is massive adoption of work-from-home tools and a greater usage of cloud services. This makes it further challenging for cybersecurity leadership as they find ways to maintain the security of their informational and business assets with offsite and onsite employees.

**What are the New Cyber Security Challenges Now?**

The coronavirus pandemic has introduced new challenges for cybersecurity leadership. Let’s have a look at some of them.

* Social engineering attacks have become more effective and easier as a result of workforce that is spread across onsite and offsite locations
* Specifically designed for identifying irregular patterns, Security Operations Centers (SOCs) are now left with partial visibility
* Increased dependency on personal devices and home networks has paved the way for numerous cyber-attack vectors
* Ransomware attacks have found new vulnerable targets in the form of hospitals and healthcare services with more frequent Denial of Service (DoS) attacks

Keeping these challenges into picture, cybersecurity leadership needs to move past compliance metrics and work for a shared ownership in their organizations. The major challenge lies in protecting the infrastructure and digital assets while simultaneously ensuring uninterrupted operations. Hence, cybersecurity teams now have to adjust their security and risk management programs to allow for adoption of work-from-home tools and cloud services.

A report by World Economic Forum titled “Cybersecurity Leadership Principles: Lessons Learnt During the COVID-19 Pandemic to Prepare for the New Normal” proposes five principles for cybersecurity leadership for balancing goals in the short-term with those in the long-term.

1. **Fostering a Culture of Cyber Resilience**

The digital environment exists in a very dynamic ecosystem. Hence, often it happens that the threats arise and develop way before a respective regulation. To avoid this during this pandemic, it’s imperative to keep incident response and business continuity as priority. Employees need to be taught to be more cyber resilient than ever before. Organizational security should be seen as everyone’s responsibility. Thus, security leadership needs to ensure that this responsibility is met by training the employees regularly on how to identify scammers, phishing attempts, [credit card](http://www.cardzgroup.com/SmartTokenBands.html) frauds and malware prevention. They also need to be educated about all the new techniques deployed by cyber attackers during this pandemic.

1. **Protecting the Critical Assets and Services of the Organization**

The cybersecurity leadership needs to have a holistic and systemic view of critical services, applications, suppliers and assets for determining potential consequences that may result out of any crisis and impact the revenue, employees, service continuity and customers. Thus, they need to maintain an account of their digital assets for ensuring effective vulnerability management program. A layered access mechanism should be in place which allows only privileged users to access sensitive information.

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

As risk posture of businesses has changed significantly, cybersecurity leaders should balance risk-informed decisions post-covid. As the retail and jobs market drastically changed, there was a sudden rise in development of new applications to cater to the changing needs. Thus, many of them were rolled out hastily while still having bugs and configuration issues. These applications can be threatening to the supply chain of organizations, as hackers can easily identify and exploit vulnerabilities in the value chain. It’s important to take informed decisions during the entire supply chain process.

1. **Updating and Practicing your Response and Continuity Plans as your Business Transitions**

Crisis management is the key of every business continuity plan. An organization that only focuses on analyzing and mitigating its risks is usually unable to effectively handle sudden and unanticipated crisis. In a crisis as big as this, we need to have cross-functional teams along with detailed plan for orienting employees with diverse roles. As digitization is continually accelerating at a fast pace, we need to adapt cyber risk with agility and speed, and align it with strategic priorities and risk appetite of the business.

1. **Strengthening Ecosystem-wide Collaboration**

The public and private sector leadership needs to collaborate and participate in initiatives that secure the ecosystem from current and newly-emerging cyber threats. Furthermore, organizations also need to bring their suppliers on the same page for effectively implementing cybersecurity controls, thus encouraging regulatory alignment of third parties.

1. **Moving to No-Trust Operational Model**

In a post Covid-19 world, leadership should adopt no-trust identity and access management process. According to a Trust Progress Report of 2020 by Pulse Secure, [72 percent](https://www.pulsesecure.net/resource/2020zero-trust-report/) of organizations were in favor of assessing and implementing Zero-Trust policies in order to mitigate cyber risks. This concept relies on continuous authorization and verification and not trusting any of the stakeholders, including the end users. As part of this model, organizations should implement security protocols such as biometric technologies and multi-factor authentication to reduce the threat of attacks.

1. **Securing a Remote Workforce**

In most organizations, the remote workforce trend is here to stay for a while. According to a research by ESG, [79 percent](https://www.esg-global.com/blog/10-security-changes-post-covid-19) of executives in the IT industry say that they will be flexible about Work from home practices even after the pandemic is over. This requires strategic changes to security initiatives by cybersecurity leadership.

They must secure remote connectivity by implementing layered defense that can detect suspicious activities from a remotely connected endpoint. In order to reduce the time it takes from detection till mitigation, organizations should invest in solutions that can increase their capability of monitoring and quick response. As a result, they can monitor employees, collaboration tools and third parties remotely and identify abnormal activity in a timely manner.

**Conclusion**

It cannot be expected of cybersecurity leadership to be able to achieve flawless security in current scenario. Still though, effectively managing cyber risk can allow businesses to achieve better and faster transformation to stay ahead during this time of uncertainty. In the end, resilience is the key to surviving through it.