Octal0g1k

ANSWERING YOUR CYBER CHALLENGES

Cybersecurity: Managing the Risk & the Opportunity

> *"An ounce of prevention is worth a pound of cure.*
>
> *Benjamin Franklin*

Cybersecurity – The Importance

Cybersecurity is today a lever for competitive advantage in a world accelerating forward with intense digitalization. Along with being a shield that protects organizational innovation and intellectual property, it is foundational to digital trust, market making, and inclusivity. The state of cybersecurity is now a concern that transcends the interests of the any organization and holds the attention of executive management and the board.

Data triumphs everything'. The one who controls data; controls people, controls governments, controls the future. The most vulnerable link in today's times is "Breach of Data" and the biggest investment in the entrepreneurial mind is 'How to secure Data Breaches?', because once data is compromised, confidentiality, integrity or availability are compromised.

COVID-19 changed how we work, shop, and interact. Lockdowns accelerated the rise of remote work, and 'DATA' became the center piece of the 'New Normal' which became the buzzword of the year. In 2020, credential stuffing attacks gained in popularity and sophistication due to the COVID19 situation, which increased the use of collaboration tools, such as WebEx and Zoom.

Globalization that had transformed the economic markets into a strongly interconnected system at the international level, came to a standstill. Critical links in the global supply chain were broken, supply chain disruption rippled across every industry. Consumer fear, bottlenecks, and shipping delays created surges in demand and shortages in supply. All these risks for companies aggravated during COVID19.

Cybersecurity ecosystems have seen the toughest ask from entrepreneurs, governments and most importantly citizens. Cybersecurity has scrambled to manage the 'New Normal'. The opportunities for profiting from espionage, IP theft, ransom, and other criminal activities increased while the world directed their attention to the clear and present danger of COVID19 have been immense.

As more and more organizations adopt cloud, automation, and digital transformation and prepare themselves better for future disruptions, the need for a secure cyber foundation has never been stronger.

Cybersecurity: The Threat and The Risk

Every year, new strains of malware emerge that attempt to exploit weaknesses in Enterprise IT defense mechanisms. While threat-hunting teams pool their energies toward identifying new persistent threats that are sometimes undetected by traditional toolsets, most Security Operations Center (SOC) teams need to also deal with the volume of regular threats that slip through the weak links in a layered defense. These cyberweapons cannot be ignored and consume SOC resources already crunched for time.

Obtaining confidential information without the information holder's consent has serious business implications because the stolen data generally includes intellectual property, personally identifiable information (PII), or financial data.

Cyber threats continue to evolve, dovetailing with the emergence of new technologies and attack surfaces. The cybersecurity industry has, mostly, responded with technology controls that can help prevent or detect such risks as they materialize. However, what continues to be the elephant in the room is the human dimension of the cyber problem. Organizations continue to grapple with how to protect the first line of defense. For example:

1. Ransomware continues to be an integral part of an attacker's strategy. It managed to shake up a few things. Trojans continue to be the most favored agent to launch malware attacks. Organizations need to minimize the availability of system/asset landscape data in the public domain and increase efforts to improve cyber hygiene. Worms, a tried and tested technique for attackers, are always an attractive malware type.
2. Cryptominer attacks have continued to dominate and the majority of attacks belong to this category. This technique has lured attackers to use it for financial gains. Also, attackers can easily embed cryptomining capabilities into the compromised machines handled by them, making these attacks a preferred choice.

The hard truth is that this new reality has only exacerbated the status quo for cybersecurity professionals. Security leaders were already struggling to address the challenges of today's fluid network boundaries. This is now exponentially compounded as millions of workers connect remotely to corporate networks while working with critical data that has moved seemingly overnight to newly deployed software-as-a-service.

Cybersecurity Regulations:

Laws and regulations play a pivotal role in the cybersecurity environment, helping shape rights, obligations, and behaviors. Thus, regulatory changes can have a macro-level impact across jurisdictions. Legal directives across the cybersecurity landscape are changing around the globe. More countries are adopting methods of imposing huge fines for non-compliance to data protection laws. Countries across the globe are responding to citizen concerns, consumer demands, globalized trade imperatives, and geopolitics to strengthen their privacy and data security legal regimes every year.

Mitigating cyber risks involves establishing organizational policies ranging from employee behavior to technical security controls. At a minimum, the organization must achieve compliance with applicable regulations as GDPR, and industry standards, such as PCI DSS. So beyond ensuring compliance, leaders must consider and manage risks that apply to them based on the nature of the business, the scope of operations and so forth. This also means adequately funding cybersecurity resources consistent with a plan that implements critical security controls (like the CIS Controls).

It is important to ensure that the means of complying with legal obligations align with business objectives and areas of real risk; cyber security management should not be a box-ticking compliance exercise.

Cybersecurity: Governance & Resilience

Enterprise security governance goals must be aligned to corporate governance objectives to manage risks through the effective rollout of control measures. For organizations to achieve continuous cyber resilience, they need to assess maturity at the point of departure and draw short-term and long-term strategies to predict attacks, protect from attacks, detect intrusions, and activate timely response and recovery mechanisms. In addition, the role of government agencies in aiding the private sector against state-sponsored attacks will be increasingly under scrutiny.

In the COVID-19 scenario, the cyber resilience framework had undergone stress tests as threats, events, and incidents will need to be identified and mitigated. A cyber-resilience framework that provides mechanisms for communication of roles and responsibilities, feedback, and critical imperatives between various layers of the enterprise hierarchy is urgently needed. Cyber- resilience is required to prove itself across dimensions of assessment of cyber risks and threats; prevention of cyberattacks and response mechanism to cyberattacks.

Post COVID19:

Ready or not, enterprises today have to manage a new normal that includes a distributed workforce and new digital strategies. A major trend over the next 6–12 months will be preparing companies to secure their employees and brand in the new normal.

The world post-COVID-19 will look much different than it did just a few months ago. There will be employees that never return to the traditional office, with businesses having had their eyes opened to the fact that they can operate securely without being in a building.

There will also be businesses that do return to working side-by-side with their colleagues but with the understanding that disruption could happen again and that they must be equipped to quickly and efficiently switch back to working remotely.

Cloud adoption, digital transformation initiatives, and hyper-automation are expected to accelerate in the post-COVID-19 world. Cloud-enabled scalability and automation can address the need for future business resilience during similar disruptive situations. However, rapid migrations of enterprise services to the cloud need a secure foundation.

Zero trust architecture will play a critical role in managing threats as organizations shift their traditional approaches to keeping data, people, and systems secure. In zero trust-centric approaches, the trust zone is compressed to narrow segments where continuous decision-making occurs. This approach works under the assumption that the threat actor is already present in the environment.

Cybersecurity: The Future

Strong collaboration between the public and private sectors is a necessary enabler for identifying new threats in cyberspace and evolving strategies to counter them. Collaboration becomes even more pertinent when it comes to protecting 'Cyber Critical Infrastructure'. Shared responsibility is the foundational principle in cybersecurity. Information sharing between organizations in the private sector directly or through government intermediaries is critical to stay abreast of threat actor actions.

The future of cybersecurity is indicated by the high number of patents filed in the 'data security' and 'device security' areas followed by 'network security'. With the rise and growth of emerging technologies such as Artificial Intelligence and Machine Learning (AI/ML), the use of these technologies will rise in both cybersecurity practice areas and their widespread adoption.

The emergence of Decentralized, consensus-based identity verification solutions; gain in Serverless security; computer vision and ML-based identify verification; and Internet of Things (IoT) device security solutions using quantum driven key management are some of the promising areas in Cybersecurity.

Thus, as more and more cyber threats emanate from nation-state actors, the home government's role and military doctrine around cyberattack response would play a critical role in protection of 'Cyber Critical Infrastructure' and the engaged collaboration and cooperation between all actors of cybersecurity would remain a key to protecting our citizens and our nations.