SOPHOS
Cybersecurity evolved.

Synchronized Approach to Modernize Cybersecurity

Industry Context

Traditional corporate cyber security has come under scrutiny in today's dynamic economic and social regulatory environment. Practices that were established when data applications and other elements of IT infrastructure were located within a company's four walls, are now unfortunately not sufficient for an era characterized by cloud computing and increasingly decentralized threats.

What we call as the more hyper-connected boundary-less network is the new normal for a modern digital organization. The current times opens up wider threat surface and numerous vectors for elements with ill-intent across the world. So, technology advances from the internet of things to AI and advanced analytics are enabling purpose-driven, resilient and adaptable enterprise. Yet, the challenge remains for many companies where IT cyber security principles and tools are still an afterthought, continually trying to catch up to the technology disruption.

As a result, while business keeps focusing on rapidly pushing new products to the market, the necessary security standards and governance frequently lag behind. At the same time, cyber-attack risks faced by companies using dated security methods have been intensifying in recent years; and these challenges have dramatically increased with the advent of the COVID -19 pandemic.

So, with a significant portion of employees working from home, sensitive data such as employee information, IP, corporate financial data, customer data and other proprietary information needs to be frequently shared outside the company's four walls. Consequently, the digital ecosystem continues to evolve, meeting the growing the need for frictionless interaction with customers, and this may sometimes lead to compromise on security, leading to irreversible reputational and financial damage.

Witnessing a Diametric Change in the Threat Landscape

The pandemic months have definitely been a period that can well be termed as a 'cyber pandemic'. The times have experienced a work from anywhere transition and pushed companies to drastically change their way of operations and move to a wholly different mode of transaction. This has been true for industries across the board, including sectors like manufacturing that traditionally regarded remote working as non-existent in their area of business.

Therefore, the pandemic has put the spotlight on numerous quotients such as adaptivity and the role of IT in being an enabler to business continuity. The agility and responsiveness of companies to acclimatize to the new ways of working has become indispensable for sustained and secure business success- both from a people perspective and equally from a security infrastructure standpoint as well.

The last couple of months have also propelled a shift in culture and mindset of organizations. The pandemic has in fact allowed security leaders to better articulate the risks and hostility of an unsecure environment and create stimulating conversations on why unwavering focus is needed on ramping up security infrastructure investment, which can go a long way in protecting them against cyber havoc.

Organizations have also witnessed a cultural shift wherein internal as well as external customers are becoming increasingly aware of what security means to them, and are readily equipping themselves with practical knowledge to circumvent security threats- both at home and at work. Now, security no longer remains confined to one particular department or function or even the four walls of the organization but rather, it has become an overarching priority. With heightened cognizance at play, users and customers are taking pride in become 'security ambassadors' to protect oneself and their organization as well.

In a nutshell, security is the focus and will continue to remain an evolving subject. How well organizations remain well-versed in employing best practices to navigate seamlessly for safe delivery of business coupled with relentless focus on health of staff will determine their success story.

Balancing Priorities for Diverse Companies

Given the current landscape, a zero-trust approach that is underpinned by greater verification modules is imperative in today's high-threat ambiance. This can go a long way in charting out a strategy that leads to a healthy and synchronized security environment and pays utmost attention to content handling access controls and overall awareness around need for enhanced security.

If businesses are following best in class cyber-aware practices, then they are well placed to manage both perimeter security as well as data security. The crux of the matter is that balancing priorities really boils down to a mix of technical expertise combined with strong internal processes.

Combating Advanced Threats in a High-Volume Environment

A high-volume environment poses multiple challenges. As an example, companies with massive volumes see incoming attacks at a humungous velocity of around 200 attacks a minute. Therefore to circumvent security breaches, organizations must have a distinct focus that is well summarized as 'outside-in' and 'inside-out' control mechanisms.

Organizations must acknowledge that the attack methodology is constantly gyrating and it vastly differs from business to business and location to location. Teams must understand that attack patterns are constantly changing and therefore, the first step to creating an invincible environment is recognizing the nature of attacks, patterns and methodologies, and accordingly craft processes and technologies that become preventive barriers to cyber-threats.

It's important to remember that qualitative analysis is not enough to create counter strategies, however there are certain advanced technologies that can enable organizations with threat intelligence. The new normal is all about understanding the nature of attackers and then defining the most appropriate security strategy based on regulatory requirement, contractual obligations and own policies.

In fact, building a secure environment

starts with something as basic as email security.

Devising Secure API Strategies

The first and foremost step to designing a secure API strategy depends on how well the organization has visibility into the number of APIs they hold. Following a zero-trust approach that keeps verification embedded in all actions, coupled with end-to-end knowledge and awareness becomes imperative. This has been made possible through advanced security technologies built on technologies that encompass AI and machine learning.

Along with visibility, it's equally important to cultivate a culture of security within the organization. In today's day and age, the demarcation between personal and professional security is fast fading. Therefore, security is a practice that must be incorporated holistically. It has been observed that internal customers, who sometimes are the weakest link, must be strengthened to empower the organization with a superior and secure barrier against cyber-threats.

Key Benchmarks When Evaluating Security Solution

When it comes to the topic of creating a secure environment, it all boils down to laying a solid foundation with hygiene practices both at the technical level (antivirus patches, next generation firewalls, multi-factor authentication) as well as at the process level (access reviews, change management reviews, admin practices, incident management). It's also important to be attentive towards identities and access management, given that identity today has become the new perimeter.

One of the prime considerations that cyber security leadership believes is absolutely non-negotiable is the aspect of 'never trust and always verify' and of course following the rules of the land such as compliance guidelines by Reserve Bank of India (RBI), Insurance Regulatory & Development Authority (IRDA), General Data Protection Regulation (GDPR), to name a few

When choosing the right solutions, it's beneficial for organizations to partner with providers that have a shared value system in terms of security, ethics and compliance. In essence, thecy ber security partner should be at least as adaptive as the customer organization and should definitely reflect some level of 'as is' in terms of capability, technology, culture, people, mindset and overall background.

Another best practice can be for businesses to set up a smart security operations center. For small to mid-sized organizations, such an SOC can be outsourced to reap the benefits of latest security technologies and intelligence, while they continue focusing on their core competency. This can vastly enable organizations to jumpstart their journey towards securing their ecosystem with increased visibility and tailored action-plan.

All these varied ways of working should then be topped up with relentless focus on creating awareness around secure practices, not simply limited to employees or internal customer base, but rather extending it to the entire ecosystem of developers, system admins, partners and suppliers. Thus, pandemic is a clarion call for a shift in mindset to a more secure way of thinking and doing.

Conclusion

A key takeaway for organizations is to remember to hold relentless focus on cyber-security. So, the philosophy and practices on cyber security must change and become more robust, modern and designed to be adaptable, risk-based and context-aware. The need of the hour remains on touching base with various aspects of cyber-security strategies that need to be harmonized. And this is where cyber security must be headed towards creating synchronized and synergized ecosystem of developers, users and customers, leading to an emergence of an invincible environment for one and all.