In This Edition

CISA’s Strategic Plan: A Step in the Right Direction

Organizations Should Break into Their Own Networks

The Fight Against Fraud Continues

...and much more...
The Art and Science of Building a Cyber Security Tech Stack

How companies should approach assessing risk and vulnerabilities and build cybersecurity tech stacks that address their unique needs in terms of protecting company and customers’ data

By Camellia Chan, CEO and Founder X-PHY

The pandemic, the ubiquity of cloud computing, and the increasing convergence of online and physical systems have accelerated the transition to online business functions in almost every industry. As CISOs and other leaders have strived to keep security initiatives up with the digital transformation, they have deployed collections of solutions for data loss prevention, endpoint security, access management, and more. A properly constructed cybersecurity ‘tech stack’ works in concert with employee education to form a successful cyber risk management program. However, IT and data security leaders face an imposing task in revamping or constructing their cybersecurity tech stacks because of the increasing sophistication not only of criminals but also of our own developing technologies. How should companies approach assessing risk and vulnerabilities, and build stacks that address their unique needs in terms of protecting company and customers’ data and defending against malware and ransomware threats?
More devices + more tech + more data = more cybercrime

Accenture reported in 2021 a 125% year-over-year jump in cybersecurity incidents. Despite growing awareness and a wide variety of more advanced tech tools, the criminals are stealing more every year, costing an estimated $3 trillion annually. More devices, more data, and more remote workers mean more opportunities for cybercrime, the most prevalent of which are malware, ransomware, social engineering, and distributed denial-of-service (DDoS) attacks. Bad actors are expert at zeroing in on the smallest security gaps, exploiting vulnerabilities in identity threat detection, endpoint protection, cloud-based supply chain, and socially engineering attacks that prey on employees with poor cyber hygiene.

With every business function having multiple tech solutions working simultaneously, IT and security leaders can understandably feel overwhelmed by integrating a cyber tech stack into 50 or 100 other software tools. A typical midsized organization employs somewhere between 10-15 solutions in its cybersecurity tech stack. The first step is realizing there is no one size fit all security stack. CISOs must carefully choose offerings and configurations that address both their specific needs and the gaps in their cybersecurity systems.

Mind the gaps in building a cybersecurity tech stack

With thousands of products and just as many vendors in the market the process can easily get out of hand if not approached from an organization-first perspective. A typical cybersecurity tech stack may include solutions for network infrastructure, identity and access management, endpoint, application, threat intelligence, and more. The cybersecurity chief should collaborate with management across departments to make sure the security program aligns with business objectives. Business leaders who view cybersecurity as a reactive cost-center are ignoring considerable business benefits that data security brings, from cultivating customer trust to creating better employee user experience. The security leader should build a risk profile that includes budget, manpower and technology knowledge. A detailed risk profile checklist identifies threats and vulnerabilities to determine the probability of an exploitation and the resulting impact on the organization.

Armed with this assessment, the CISO can select software solutions that address the specific gaps within existing systems. The company can design a cybersecurity infrastructure which will be multi-layered and diversified, addressing risks across the enterprise from physical hardware and internal software to external vendors and the network perimeter. Once the technologies have been selected, an organization needs to create a sound strategy for implementing and integrating the cybersecurity tools into the IT infrastructure, careful not to implement too many at once and thoughtful about which vendors to select. Gartner reported one of the top cybersecurity trends is currently the move toward vendors that consolidate multiple security functions into a single platform, which may reduce complexity, cut costs and improve efficiency.
Avoid tech Jenga with the right stack

Companies should avoid using multiple layers of one form of protection. They should diversify them across the system to provide a more holistic barricade against cyber threats, securing each layer of the system, one on top of the other. Single layer solutions are no longer adequate to protect against cybercriminals. Too many organizations are still relying solely on reactive, software-based defenses instead of a comprehensive multi-layer approach that includes the often-neglected hardware and firmware layer. Once implemented, the cybersecurity tech stack can mitigate risks that are plaguing American business, making it as difficult as possible for hackers to intrude, enabling better defenses for a distributed workforce, rising to meet the ever-increasing sophistication of attacks, and bolstering that last line of defense, physical hardware. However, the most fortified cybersecurity tech stack in the world will not thwart all threats, since human behavior accounts for over 80% of incidents. Phishing and other forms of social engineering attacks are the most common threat vectors, making a comprehensive education and awareness program an absolute necessity in securing an organization's data.

Stacking the deck against cybercrime

As the sheer volume of data and digital transformation continues expanding, so do our vulnerabilities. Most business leaders now recognize the necessity of cybersecurity vigilance, since cyber-attacks at best cause lower profit margins and at worst can prove catastrophic. While developing a powerful cyber defense tech stack has become essential, leaders must not only focus on the technology but also people, strategy, plans, and training. Companies that discard the obsolete view of cybersecurity as a reactive cost center and make it a cross-functional priority will gain competitive advantage. If company leaders work together to assess risks, find the weaknesses, and build a tech stack that directly addresses the weaknesses, they can make cybersecurity a revenue driver, a differentiator, and a trust generator.

About the Author

Camellia Chan is the CEO and Founder of X-PHY, a Flexxon brand. Since its inception in 2007, Camellia has grown Flexxon into an international business with a presence in over 50 cities. With Camellia’s passion for innovation and tech for good, Flexxon continues to expand its essential suite of cybersecurity services through its flagship X-PHY brand.

Camellia can be reached online at @XphySecure and at our company website: https://x-phy.com/