Effective Cybersecurity is Essential as Cyber Threats Expected to Continue Over Next Decade

At a Glance

Cybersecurity is recognized as a top enterprise risk. For organizations to harness the power of effective cybersecurity frameworks, they should:

- Understand the latest technologies and approaches shaping security programs
- Build resilience into the framework
- Monitor, detect and respond to cyber incidents with agility and speed
- Collaborate effectively across the C-suite

Cyber threats are among the top ten highest-rated critical risks of organizations today and for 2030, according to Protiviti's Executive Perspectives on Top Risks for 2021 and 2030*. The constantly changing risk environment requires companies to be agile in how they adapt and address cyber risks. CIOs and CTOs often transform business solutions to enable the business using tools such as artificial intelligence (AI) and* Internet of Things (IoT)*. But with these tools comes new or increased cybersecurity and technology risks.*

Without clear communication of the business risks and threats to business success, actions taken to manage cyber risks can create inherent conflict within organizations, increase competition for funding and resources, and create a perception that runs counter to business enablement. Having an effective change management program, initiated and sponsored by senior leadership, changes the tone at the top and can promote acceptance of the processes and policies put in place to manage cyber threats.

Moving off legacy platforms into more agile technology environments such as Microsoft Azure (and other cloud providers) enables organizations to safely benefit from the opportunities that such tools bring. When approached in a thoughtful and disciplined manner, organizations can accomplish their transformational objectives while, at the same time, taking notable steps to improve their security posture.

As organizations continue to modernize their technology platforms, key cybersecurity disciplines and approaches need to be considered.

New approaches to data protection

One of the key technology shifts that has shaped cybersecurity programs is the move to cloud (i.e., XaaS). This has drastically impacted the efficacy of traditional cybersecurity technologies, thus forcing organizations to evolve and update their cybersecurity architectures. It also has led to a de-emphasis of perimeter-based controls wrapped around the corporate network as the focus shifts more to identity and data-centric approaches. Capabilities such as micro-segmentation, Secure Access Services Edge (SASE) and software-defined perimeters are now needed to securely enable employees and conduct business with customers. These new approaches have proven especially effective as many organizations pivoted their operations to remote work environments. While endpoint devices such as laptops and mobile devices will play a role in organizations for a long time to come, these new architectures are required to extend traditional controls out and away from the protection of corporate networks to any location around the world. As organizations introduce new technologies during the course of transformation, it's important for the CIO to understand potential risks and plan for the right management of these risks.

Resilience as a foundation

Resilience is another key to success within cybersecurity programs. Modernization of an organization's technology platforms represents a significant opportunity to build resilience into the key applications and infrastructure that support core business services.

When no longer constrained by legacy platforms and outdated technologies, organizations can leverage a variety of new and evolving technologies like the cloud to significantly decrease the likelihood of a sustained outage with business impact. From high-availability architectures to enhanced workload and service management, CIOs must take a thoughtful and intentional approach to capitalize on the opportunity and build resiliency into the go-forward architecture. Speed, funding and pandemic-supporting operations, however, are preventing these changes from happening quickly. The IP that exists in outdated technologies remain in place and serve as the basis for many company operations. It is also important to note that some areas of a business, such as assembly lines (some of which are FDA certified) are unable to legally move quickly to adopt cloud and replace legacy applications.

Visibility, speed and agility

Much has been written about the zero-trust architecture, and while there is no shortage of opinions on the topic, one aspect that many cybersecurity practitioners tend to agree on is that experiencing a security incident is not a matter or "if," but "when." Zero trust as a security model has started to catch on because one of its core philosophies is to always assume that adversaries are in an organization's environment. This is a significant mind shift from how programs have historically been built. This shift not only impacts how a program is designed, but where and how budget is applied. An "assume breach" philosophy will push an organization to turn from heavy investment in preventative controls to a more balanced portfolio that includes an emphasis on visibility and response.

Organizations can minimize cyber risk exposure and incident impact to business operations through enhanced monitoring, detecting and response capabilities that feed an organization's agility and speed, support resiliency, and potentially reduce adversary dwell time. CIOs should plan ahead for transformation to create more resilient services that enable business operations.

Engage with the C-suite

Cybersecurity has implications that ripple across the entire organization. All C-suite members must understand their roles in the company's cybersecurity risks and ensure appropriate cybersecurity oversight in their respective operations and transformation projects. CIOs who collaborate with their executive counterparts recognize that while CIOs drive many cybersecurity decisions, joining forces with the rest of the organization's leadership team helps solidify technology implementation and change management while boosting ROI. Each C-suite member is uniquely impacted by cyber technology:

- **Chief information security officer (CISO)** — There is a significant reliance on IT and cybersecurity working closely together to monitor, detect and respond to cyber incidents. As large-scale attacks progress and elevate risk profiles, it is imperative that CIOs prioritize cybersecurity in step with CISOs.
- **Chief risk officer (CRO)** — Difficult investment decisions are made by CFOs. CROs must help uphold the ROI on such decisions by placing IT and security risk on a par with other enterprise risks.
- **Chief audit executive (CAE)** — To the extent cybersecurity impacts internal controls, auditors must have the proper training to audit controls in a cloud environment.
- **Chief marketing officer (CMO)** — CMOs must be well-positioned to produce a secure enablement of the customer journey, including securing customer identity and access management (CIAM).
- **Business leaders** — To build resilient businesses, leaders must take an active role in enabling IT with a strong understanding of business goals and services. Accordingly, business leaders must help contribute to recovery from adverse cybersecurity incidents.
- **Employees** — Employee buy-in through proper training and change management strategies is instrumental to cybersecurity transformation and modernization projects.

Where do companies go from here?

Cybersecurity demands agility and resilience. As organizations move through their enterprise transformation journeys, it is important that they consider the following issues to optimize ROI:

- Proper cyber "hygiene" is foundational to managing security risks and maintaining resilience of business services.
- Organizations should have a clear maturity assessment of their current cybersecurity protection, with the target maturity level agreed on by both the CIO/CISO and top executives or the board. This will allow the CIO/CISO to plan for future improvement.
- Companies must mitigate cybersecurity risk without slowing down enterprise transformation and should search for opportunities to boost enterprise value with novel tools such as Greenfield cloud environments.
- CIOs and CISOs should evaluate the extent of cybersecurity implementations with an eye on enterprise transformation, carefully determining the measures required for minimally viable products or services and adding greater cybersecurity complexity where needed.
- With cyber threats expected to be among the top ten risks for organizations across the next decade, CIOs must ensure that their organizations have effective cybersecurity programming to mitigate risk and protect their company's valuable assets during and after digital transformation.

AUTHORS

MICHAEL PANG, Managing Director, Technology Consulting, Hong Kong
NICK PUETZ, Managing Director, Security and Privacy, St. Louis
ANDREW RETRUM, Managing Director, Security and Privacy, Chicago

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

For more information, please contact us at TechnologyConsulting@protiviti.com.