CYBALT

What are the Key Risks of Digital Transformation?

Cybalt Inc. Suite #510, 2701,
North Dallas Parkway, Plano, TX

discover@cybalt.com

What are the Key Risks of Digital Transformation?

Organizations face a drastic change in the working culture and growing business needs. Because of this, they need to embrace digitalization and aim for a significant transformation of their business and operating models, overcoming all kinds of constraints driven, for example, from creeping legacy IT systems, siloed business divisions, central support functions, and the cultural resistance in a constitutionalized industry.

Market report suggested that through the pandemic, customers have gained better access to products and services at the click of a button than ever before. The bar for delivering exceptional digital customer experiences is high – and is set to get higher. This hyper-connected world will likely face expanding cyber risks on multiple global fronts due to the digital shifts created from the pandemic – remote, secure work environments, digital engagement, and customer service.

The translation is a big CISO challenge: explaining risk dynamics to the board and operating committees in collaboration and cooperation. They should articulate that they're not trying to stop the business instead of supporting enhancing the trust of their consumers, investors, and partners. Security should be a shared responsibility model, owned by everyone.

Considering the current situation, below are a few risks and challenges we have identified regarding digital transformation.

Increasing the scope of the strategic security discussion Cyber security leaders must strategize and modulate their conversation from cost and speed to adequate security to help deliver enhanced business value and user experience. Senior leaders must understand that managing cyber risk is vital for competitive advantage and long-term success. CISOs and their teams should help leadership realize what goes into cyber security and the importance of privacy by designing better to align security with the organization's strategic business objectives.

1. Talent and skill sets that are critical

Modern security programs, managed by forward-thinking security teams, are increasingly demonstrating their capacity to help firms move quickly, expand, and improve customer experience. CISOs and security executives must understand that the security team is responsible for more than just governance, security operations, and red teaming; it begins from the very beginning of development, security, and operations (DevSecOps). It needs to be ingrained in the software development process (SDLC). In general, cyber professionals should continue to develop their abilities in system-based, strategic business orientation. They must embrace a multi-modal approach that emphasizes standardization, automation, and data analytics.

2. The industry is shifting rapidly to the cloud

The terms "cyber security" and "cloud security" are synonymous. The deployment environment is the sole difference. Data protection, identity, and access control, infrastructure, and vulnerability management are all principles that CISOs have talked about for years, and they all apply to cloud security. The technology stack is what sets it apart. From implementation to monitoring and repair, the environment in which these security controls are used necessitates high automation. CISOs and their teams are encouraged to interact with business partners to ensure that everyone knows cloud-specific security needs and avoids misconfigurations.

3. Putting identity at the center of the zero-trust strategy

The zero-trust model and architecture can't succeed without placing identity at the center. Developing the zero-trust road map around identity to facilitate adoption and strengthen ROI is a crucial success criterion for a new age security program. The emergence of zero trust represents a shift in thinking in which the cyber team thinks system access is compromised and bases security decisions on identity, device, data, and context. An automated strategy reduces an environment's attack surface, establishes cyber rules and principles, and eliminates costly and inefficient manual operations.

4. Taking advantage of security automation

Many individuals feel that automation is a universal panacea, but experience has proven that a practical implementation method has the best outcomes. Organizations don't have consistent control over software versioning and the general features accessible in the cloud environment when they move to the cloud. Automation has been critical in safely analyzing risk and, as appropriate, implementing additional baseline characteristics. Unintentional data exposure, mishandled account permissions, insecure network connections, ransomware attacks, and other dangers are critical problems for enterprises in multi-cloud setups.

5. Defending the right to privacy

The progress of the regulatory environment around data privacy is being observed in near-real-time. Governments and authorities are beginning to recognize that data breaches are only a tiny part of the larger universe of cyber occurrences. The progress of the regulatory environment around data privacy is being observed in near-real-time. Governments and authorities are beginning to recognize that data breaches are only a tiny part of the larger universe of cyber occurrences. Privacy programs of the future must incorporate privacy-by-design thinking, which isn't just a philosophy; it's a cultural mind-set and an organizational shift. Data protection will be more effective when a multi-faceted approach with the cyber security, technology, and regulatory teams is aligned.

6. Defending beyond the lines

Most businesses are no longer the single, monolithic organizations that many customers formerly thought. They rely heavily on a reliable supply chain and various traditional and non-traditional partners that frequently have direct access to business systems and data. Although regulatory standards and mutually agreed-upon security frameworks can help mitigate the impact of third-party cyber threats, participants in these complex ecosystem structures — cloud providers, SaaS companies, Internet of Things (IoT) device manufacturers, and so on — may lack clear obligations for implementing adequate controls to protect their partners' data, leaving the entire network vulnerable to cyberattacks.

Conclusion:

In the future, the hyper-connected innovative society will almost certainly confront heightened cyber dangers from a variety of emerging threat vectors on various global fronts. The advancements in technology that power commerce, communications, and entertainment bring new risks. We should look into the issues such as the evolution of the security team, the automation of the security function, data privacy, and ecosystem security regularly. While none of these topics are very new, we believe they will quickly become essential emphasis areas for cyber experts in practically every industry.