www.pipelinepub.com
Volume 19, Issue 7

Mitigating the Risks of Digital Transformation

By: Srini Addepalli

Digital transformation has brought about a significant change in the way enterprises function by leveraging technology to fundamentally alter the way businesses operate, interact with their customers, and manage their operations. The boom in hybrid work across enterprises initiated by the pandemic has shifted digital transformation from a key priority to mission critical.

With digital transformation, businesses can gain a host of benefits, such as automating routine tasks, optimizing supply chain management, using AI-powered chatbots to handle customer service interactions, and enabling employees around the world to work together on projects in real time. The increased adoption of automation and support systems has allowed businesses to streamline processes and improve efficiencies, which in turn is leading to higher productivity, reduced costs, and better customer experiences.

According to a study by Deloitte, companies that invest in digital transformation are more likely to achieve their strategic goals and outperform their peers. The study found that digitally mature companies are 64 percent more likely to achieve their business goals than their less digitally mature peers. Additionally, the study found that digitally mature companies are more agile and can respond more quickly to market changes.

While digital transformation and new technologies offer several benefits to businesses, however, they also present new risks that must be addressed to ensure a seamless transition.

Cybersecurity risks

It's no surprise that one of the biggest risks associated with digital transformation is cybersecurity. The COVID-19 pandemic accelerated digital transformation to enable employees, partners, and suppliers to work remotely and collaborate over the Internet using cloud-based collaboration tools. To enable remote workers, enterprise critical applications are increasingly made available in public and private clouds. IoT sensors and actuators are also connected over the Internet to collect and exchange data to automate industrial processes. Essentially, digital transformation is making company assets easily accessible from anywhere. When systems are accessible from the Internet, bad actors can try to disrupt operations. Organizations are also embarking on application

modernization by updating legacy systems to leverage new technologies, such as microservices architecture to improve performance and scalability of their systems. Though a microservice architecture provides several benefits, it can also increase the attack surface due to multiple independent microservices.

Edge computing is one of the key enablers for digital transformation for a significant number of industries. Edge computing brings computation and storage closer to the users, providing multiple benefits including superior user experience, bandwidth savings, and compliance with the regulatory requirements of keeping data local. Edge computing makes organizations' data and compute spread across more locations than cloud computing, which increases the attack surface.

Cyber threats are a significant concern for organizations that are undergoing digital transformation. According to a report by Cybersecurity Ventures, the cost of cybercrime is expected to reach $10.5 trillion globally by 2025, so if you're not actively looking for ways to continuously protect your business, you could be putting it at serious risk. As enterprises adopt new technologies to automate processes, they are also increasing their attack surface and creating new vulnerabilities that can be exploited by cybercriminals. Cybersecurity threats can take various forms, including phishing attacks, malware, ransomware, and data breaches. These threats can compromise sensitive data, disrupt operations, and damage the reputation of the enterprise. A separate study by the Ponemon Institute found that the average cost of a data breach for companies in the United States is $8.6 million. The same study found that the average time to identify and contain a breach is 280 days. These numbers are alarming and should push all business leaders to take decisive action to secure their businesses if they haven't already done so. To mitigate the risks associated with cyber threats, enterprises must take a proactive approach. They should develop a comprehensive cybersecurity strategy that includes:

- Adopting a Defense-in-Depth (DiD) approach to stop bad actors from accessing enterprise applications via various security technologies such as firewalls, intrusion prevention systems, zero trust network access solutions, identity-aware access controls, anti-malware, anti-phishing systems, and more.
- Identity and access management (IAM) solutions to protect enterprise assets by using least privilege access methodologies. IAM coupled with multi-factor authentication (MFA) helps protect enterprise assets even in cases of password compromise.
- Encryption solutions to encrypt sensitive data to protect data from being comprehended even in cases of data breaches.
- Threat monitoring systems that conduct a regular risk assessment of digital infrastructure, applications, data protection policies, access control policies to identify potential vulnerabilities, misconfigurations, and act upon any risks identified.
- Training employees in cybersecurity on how to recognize and respond to potential phishing and other threats.

Two security architectures are worth mentioning as they are key to the success of digital transformation as they mitigate many challenges associated with cyber threats. They are unified secure access service edge (SASE) and cloud native application protection platform (CNAPP).

Unified SASE plays an important role in cybersecurity by providing comprehensive network security for enterprise assets that can be deployed anywhere—OnPrem, Cloud, Edge—for workforces distributed across the globe. SASE addresses the DiD part of the cybersecurity strategy along with CNAPP and endpoint security technologies. SASE protects enterprise data via cloud access security broker (CASB), enterprise applications via zero trust network access (ZTNA), endpoint assets via security web gateway (SWG), which combines anti-phishing, anti-malware, and site reputation filter

technologies along with basic security foundational firewall, intrusion detection and prevention system (IDPS), distributed denial of service (DoS/DDoS), and data loss prevention (DLP) technologies. By combining multiple security technologies, SASE provides comprehensive security for distributed enterprise assets.

CNAPP security technologies are becoming important too due to adoption of cloud and cloud services by digital transformation. CNAPP security includes cloud security posture management (CSPM) and cloud workload protection platform (CWPP). CSPM gives visibility into cloud assets, scanning of data for malware, and conformance to regularity requirements. It also scans for any misconfiguration of cloud services used by enterprise applications. CWPP checks for vulnerabilities in application images, malware, or unwanted software detection in images, and provides runtime workload protection via host intrusion prevention system (HIPS) and runtime application self-protection (RASP) technologies. Though cybersecurity will continue to be a concern for enterprises, especially in a challenging economy, those that take it seriously and treat it as a business enabler, rather than a costly add-on, will be most well-positioned to succeed moving forward.

Mitigating other risks

There are other risks that need to be addressed for successful digital transformation. They include employee resistance to change, interoperability with legacy systems, and vendor lock-in.

Employee resistance to change

According to a study by McKinsey, only 26 percent of digital transformation initiatives are successful. One of the main reasons for this low number is employee resistance to change. The study found that employees are more likely to embrace new technologies if they understand how the technology will benefit them and if they have been adequately trained. Additionally, the study found that successful digital transformation initiatives typically involve clear communication and collaboration between management and employees.

Integration and interoperability issues

Digital transformation typically involves the adoption of new digital systems and processes to modernize an organization's operations and achieve its business goals. However, these new digital systems and processes need to be integrated with existing legacy systems to ensure they work together seamlessly. Integration and interoperability issues can arise when there are incompatibilities between the new and existing systems.

To mitigate integration and interoperability issues, it's important to have a clear integration strategy in place from the outset of the digital transformation project. In today’s world, digital transformation is a never-ending process, so having that understanding from the start can have a positive impact on how you roll things out.

Vendor lock-in

Organizations that rely heavily on third-party vendors—including cloud providers for digital transformation initiatives—may become locked into those vendors' technology platforms, making it difficult and expensive to switch to other vendors or technologies.

Organizations can avoid vendor lock-in by adopting open standards and open-source technologies that are widely supported by the industry and avoid closed technologies and services offered by vendors. In cases of closed technologies, it is important to adopt vendors that provide data conversions to other vendors systems and open technologies.

Looking ahead

Business and technology are changing faster than they ever have, and digital transformation is a must to stay relevant with customers and to retain talent. While the benefits are well-documented, it's imperative that leaders have a clear understanding of the new risks that come along with it, and they take the necessary steps to ensure things go smoothly and that they remain protected. Cybersecurity, employee resistance to change, integration and interoperability issues, and vendor lock-in are significant risks that must be mitigated for automation initiatives to be successful.

Regardless of the risks they're facing, enterprises should take a proactive approach that includes developing a comprehensive cybersecurity strategy, educating employees on the benefits of automation and support systems, and creating a clear integration strategy at the outset of a digital transformation project. By taking these steps, enterprises can better ensure that their automation and support systems initiatives are successful and deliver the desired outcomes, including increased efficiency, agility, employee and customer satisfaction, and competitiveness.