RSA

WHITE PAPER

10 MAJOR FACTORS AFFECTING YOUR DIGITAL RISK PROFILE

Many organizations today are experiencing a watershed moment when it comes to competing in the digital era. Although most have been using technology for decades to evolve their business, today's explosion of digital opportunity has created an irresistible force for change. Digital transformation is fundamentally changing organizations, delivering benefits that range from new efficiencies across operations to innovative business models. Organizations now look to digital initiatives to improve customer experiences, optimize operations, improve margins and create entirely new products, services and business models.

Enabling organizations' new or evolving operating models is a set of common digital technologies and disciplines in various stages of deployment within the enterprise. Cloud computing, robotics and automation, data analytics, IoT, mobile products and services, and social media offer many different avenues for growth and optimization. But along with all the benefits the new digital paradigm may bring, there is an undercurrent of risk to manage. Organizations' digital initiatives are forcing them to rethink risk and security strategies.

Organizations must understand risk exposure and determine how much to invest to protect their business from digital risk while capturing the benefits of digital initiatives. The new face of business requires organizations to manage and coordinate cross-functionally in a more fluid and agile manner than ever. With the business landscape rapidly shifting, risk and security leaders may struggle to determine where to start, where to go next and how to keep a sustainable and evolving risk management strategy aligned with the business. One way to stay ahead of the curve is to look at the major factors that will affect the organization's digital risk profile.

THE 10 MAJOR DIGITAL RISK FACTORS

Type of industry, competitive markets and organizational strategies all help to shape an organization's digital future. As this future unfolds, every organization will have different factors that impact the risk profile. The fact is the more complex a business or the more complex the digital initiative, the greater the likelihood a risk will manifest. Keeping risk at bay is not the end game; it is understanding the nature of the risks, taking the right ones and managing well the ones that can stand in the way of achieving strategic objectives. Risk is a multifaceted challenge, and several key considerations factor into digital risk.

Complexity of Business

Any discussion around risk related to digital transformation should start (and end) with the business. The complexity of the organization's business model and strategy will play a big role. Digital transformation should, at its heart, bring life to an organization's business. The opportunity to expand the breadth of products and services or capture market share is ripe for the taking if an organization can move fast and exploit the digital opportunity. A complex business will require more sophisticated practices to treat risk and in turn will complicate efforts to mature the organization's risk management capabilities.

Data Profile

Digital initiatives revolve around data. The types of data involved can vary—from internal, confidential data sources to highly proprietary models to consumer and

personal information. Following the path that data takes through the labyrinth of a modern enterprise, especially one that is undergoing an accelerated expansion via digital initiatives, is extremely difficult. If data is the currency of the digital transformation, then data governance, risk assessment and protection practices securing that data must align with the type and volume of data associated with any given digital initiative.

Technical Complexity
The complexity of an organization's technical architecture has a dramatic effect on its risk profile. In this respect, it pays to keep in mind the tremendous difference between introducing new technologies and using existing ones. Although some organizations may be focused on optimizing existing processes by leveraging already deployed technology, most digital initiatives have some element of innovation. For example, automating business processes (through, for example, robotics process automation, or RPA) or implementing complex analytics and modeling can bring extensive improvements. But the risks are also considerable if the automation or analytical model leads to the wrong decisions. Technical complexity also impacts operational changes such as making a transition to DevOps approaches, ensuring skills and resources are staffed up to handle the new architectures, and inserting new technology into current risk and security operations.

Technical Stability
A related factor to technical complexity is the stability of the technology. Leveraging a known, reliable infrastructure has one risk profile; deploying the latest advanced technology has another. In addition to the technical considerations of emerging technology, such as unproven, constantly evolving and potentially vulnerable code, there is also the business aspect of building digital business models on a very fluid technology market. Acquisitions of innovative technology companies can impact strategy by adding the wild card of a vendor disruption.

Cloud Architectures
Whether it is virtualization on private infrastructure, deployment of workloads into public cloud infrastructure or the use of SaaS services, cloud technology is pervasive. The nature and scope of an organization's cloud strategy will shape how digital risk affects a wide range of business intents. Most organizations are already undergoing a shift in this area, but as digital business expands, the use of cloud architectures, visibility into emerging threats and business risk may narrow.

Technical Scope
The scope of an initiative will influence associated risk. From a security perspective, a large, expansive technology footprint expands the attack surface; from an operational perspective, it complicates the IT management surface. The use of IoT, operational technology (OT) and mobile products are obvious examples of potentially massive increases in the scope of a digital operating model. But it is not just the number of technical components, such as devices, that contributes to the technical scope. The user base related to the digital initiative is also a significant factor. As compromised credentials are the number-one threat vector related to compromised systems, the nature and number of users have a considerable security impact.

Geographic Scope
While the digital world seems to transcend physical borders, the physical location of data, users and systems does have an impact. This includes not just internal resources but also external actors such as supply chain participants, service providers and third parties. Geopolitical, legal, cultural and operational factors related to geographic scope will influence risks, especially in circumstances that involve consumer usage.

Compliance Impact
Regulatory compliance is a persistent challenge for organizations today. The scope of regulatory requirements related to areas such as data privacy, industrial and environmental impact, financial reporting and labor law must always be considered as part of digital business initiatives. Some digital initiatives may result in business and operating models whose relationship to regulation has yet to be fully understood. Emerging regulations from one or more political jurisdictions may be on the horizon for many digital business tactics.

Use of External Third Parties
The use of cloud providers and third-party specialists, including contractors, consultants and outsourced IT infrastructure, is a major part of most digital initiatives. While potential third-party risk has long been a concern for organizations, the digital ecosystem amplifies its impact. For example, several notable data

breaches have been the result of attacks originating with external parties or data being mishandled by business partners. Additionally, according to PwC's 2018 Global Economic Crime and Fraud Survey, 68% of external actors committing fraud are "frenemies" of the organization—agents, vendors, shared service providers and customers. The use of external parties also has a compliance impact as many regulations today (including EU-GDPR, GLBA and HIPAA) require good governance around third parties.

Resiliency Requirements

The very fact of migrating manual processes to digital ones increases the impact of a business interruption. For example, media organizations that once delivered publications to customers' driveways or mailboxes were subject to service interruptions from snowstorms and carrier illness. As these companies migrated to digital delivery, the risk expanded, because deliveries to the entire customer base could be interrupted by a host of threats—lost power, ISP disruption or cyber attacks, to name a few. Further, in today's ultra-connected world, the expectation of "always on, always there" prevails. From consumers who demand 24x7 access to employees who count on the ability to work anywhere, anytime, business continuity requirements are high. Depending on the nature of the digital initiative, this requirement may go well beyond traditional disaster recovery. In addition, given the intense scrutiny of events in the digital world, and the likelihood that news of negative events will go viral, handling crises effectively must be on every risk team's radar.

Wild Card: The Disappearing Digital-Physical Divide

One final factor to consider in assessing digital risk is the relationship between the digital and physical worlds. Many digital initiatives today include some intersection with the personal world. For example, autonomous vehicles and virtual/augmented reality both cross the border into the physical. However, autonomous vehicles have a different risk impact. Digital initiatives that overlap into the physical environment can add an element of safety to the traditional confidentiality, availability and integrity model. With the constant threat of cyber attack looming over all digital initiatives, any technology solution that could result in dangerous situations has a special risk profile that must be seriously considered.

CONCLUSION

Digital transformation is altering every organization's IT infrastructure, go-to-market strategy and business models. Technology is revolutionizing how companies interact with their consumers, how products are made and delivered, how employees work, how companies band together to create innovative ecosystems and capture efficiencies, and how each and every company must compete in today's marketplace. The factors that affect a company's risk profile will invariably reflect its own unique characteristics. However, the common factors outlined here will shape how organizations need to think about digital risk.

As digital opportunities unfold, companies that understand how to identify, assess, evaluate, treat and monitor risk in an effective, efficient manner will have the upper hand. Risk management practices must evolve for this to happen. A key trait of successful companies in the coming years will be the ability to disrupt risk management for the sake of successfully managing digital risk.

DIGITAL RISK IS EVERYONE'S BUSINESS, HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com

RSA