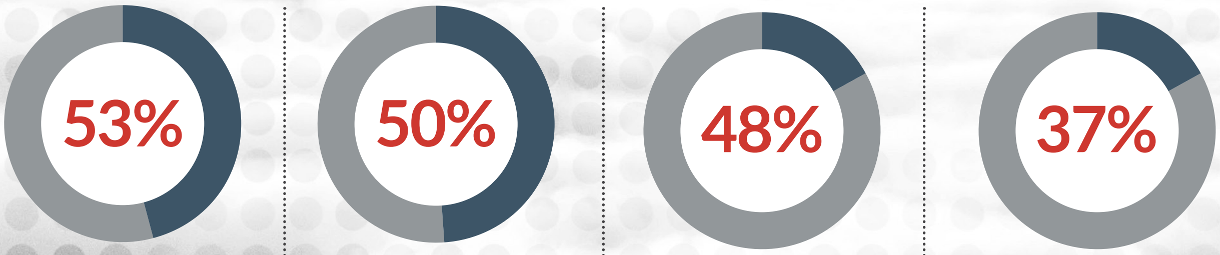
A HOW-TO GUIDE TO MANAGING DIGITAL RISK TODAY

DIGITAL TRANSFORMATION CREATES OPPORTUNITY… AND RISK

> “Today, there is no more perimeter. It’s been poked full of holes. [Organizations] need to be honest about what risks are associated with the innovations they’re adding [into their environment] before adopting it.”
>
> Dr. Branden Williams, Director, Cybersecurity, MUFG

Digital transformation is making it possible for organizations today to deliver more new products and services to more people, create more satisfying customer experiences and boost operational efficiency. But with opportunity comes risk. Digital risk refers to the unwanted and often unexpected outcomes that stem from digital transformation, digital business processes and the adoption of related technologies.

To capitalize on digital opportunity, organizations must strive to manage their digital risk. But based on the findings of the RSA Digital Risk Study,[1] a global survey of 1,050 people from organizations engaged in digital transformation, managing digital risk is proving to be a challenge. The study shows that only about half of respondents at most indicated their organizations are taking specific steps to manage digital risk.



Organizations engaged in digital transformation that have discovered or identified the risks

Organizations that have implemented process changes to reduce or treat the risks

Organizations that have evaluated or prioritized the risks

Organizations that have implemented technology changes to reduce or treat the risks

Source: *RSA Digital Risk Report, 2nd Edition*, January 2020[1]

If your organization is undertaking digital initiatives today, you’re on the right path to opportunity. To address the accompanying risks, read on to learn about actions to take to manage today’s most consequential digital risks.

EIGHT TYPES OF DIGITAL RISK

Digital transformation has given rise to eight types of digital risk organizations must learn to manage.

Eight Types of Digital Risk

Business Objectives	Digital Risks	
New Operational Efficiencies	Cyber attack risk	Risk of cyber attacks, especially in the context of a growing attack surface and an increase in sophistication of attacks
	Dynamic workforce risk	Risk related to the dynamic nature of today's workforce and the gig economy
	Cloud transformation risk	Risk due to changes in architecture, implementation, deployment and/or management of new digital business operations or IT systems
New Business Models	Third-party risk	Inherited risk related to external parties
	Compliance risk	Risk related to compliance requirements driven by new technology and the scope of data being created
Improved Customer Service	Process automation risk	Risk related to changes in processes from automation
	Business resiliency risk	Risk to availability of business operations, especially after disruption
	Data privacy risk	Risk related to the ability to protect personal information

WHERE SHOULD YOU FOCUS?
TOP DIGITAL RISKS

In the RSA study of organizations engaged in digital transformation, participants were asked to list their top three digital risk management priorities. Cyber attack risks and dynamic workforce risks were the #1 and #2 priorities for most organizations. For respondents in Western Europe and APJ, third-party risk was the #3 priority; for North American respondents, it was data privacy for the past two years, but process automation for the next two years.[1]

No organization should expect to master managing all eight areas of digital risk at one time, nor does every organization need to manage all eight equally. As you consider where to focus your organization's efforts, the priorities will depend on what risks are most consequential in your particular sector or industry, as well as what risks align with your organization's specific strategic objectives.

If you're not sure exactly which risks could be hindering your digital transformation, you're not alone. Many organizations simply don't have the staff or internal expertise to assess where to concentrate their efforts to manage digital risk. Start by learning more about high-priority risk areas from the information and links on the next few pages. The content includes detailed guidance from RSA about how to approach managing these and other selected areas of digital risk.

Figure 5: Top Risk Management Priorities by Industry (next two years)

Please think about your organization's strategy to manage the risks that may emerge or increase due to your digital transformation over the next two years. What do you believe will be your organization's most important objective? Select one.

FINANCE & INSURANCE	WHOLESALE & RETAIL	IT, TECHNOLOGY & TELECOM	HEALTH & PHARMA	PUBLIC SECTOR	ALL RESPONDENTS
Cyber Attack Risks	Cyber Attack Risks	Cyber Attack Risks	Cyber Attack Risks	Cyber Attack Risks	Cyber Attack Risks
Third-Party Risks	Dynamic Workforce Risks	Dynamic Workforce Risks	Dynamic Workforce Risks	Data Privacy Risks	Dynamic Workforce Risks
Dynamic Workforce Risks	Third-Party Risks	Process Automation Risks	Compliance Risks	Dynamic Workforce Risks	Third-Party Risks
Process Automation Risks	Data Privacy Risks	Third-Party Risks	Cloud-Related Risks	Cloud-Related Risks	Cloud-Related Risks
Data Privacy Risks	Cloud-Related Risks	Cloud-Related Risks	Third-Party Risks	Compliance Risks	Data Privacy Risks
Cloud-Related Risks	Compliance Risks	Compliance Risks	Process Automation Risks	Third-Party Risks	Process Automation Risks
Business Resiliency Risks	Business Resiliency Risks	Business Resiliency Risks	Business Resiliency Risks	Process Automation Risks	Compliance Risks
Compliance Risks	Process Automation Risks	Data Privacy Risks	Data Privacy Risks	Business Resiliency Risks	Business Resiliency Risks

MITIGATE CYBER ATTACK RISK

> “One of the biggest challenges is getting organizations to know how to protect their organization in this sort of new way of doing business.”
>
> Mike Newborn, CISO, Navy Federal Credit Union—on digital risk

Cyber risk is business risk. Protect your digital business, customer information, brand and critical assets from cyber threats.

Action Areas

Breach preparedness: Put in place technical and organizational action plans, a common language and well-defined processes, so the SOC team can contain any incident quickly, and other parts of the organization can be ready to execute specific response plans.

Risk reduction: Protect assets, address and prioritize known vulnerabilities and threats, and implement tools, policies and processes to reduce threats—with the ultimate goal of improving the organization’s risk posture.

Incident response: Be equipped to detect an attack as fast as possible and initiate the right response activities based on the level of risk the attack poses, with the goal of keeping any small incident from escalating into a major breach.

Breach remediation: Mount a well-coordinated, collaborative response, with automatic incident notification from SOC to risk managers, definition of workflows for clear communication to C-suite stakeholders and internal departments, and incident documentation to share learnings.

Post-breach adaptation: Implement processes to ensure the breach does not happen again. This can be accomplished by establishing a feedback loop on the incident and response, and then putting those learnings into practice to reduce the risk of recurrence.

MANAGE DYNAMIC WORKFORCE RISK

> “Tying back to a centralized identity source is really important.”[2]
>
> Tony Arnold, Head of Technology and Information Security Risk, ANZ Bank—on workforce risk

A growing gig economy and an increasingly mobile and remote workforce drive new workforce-related risks.

Action Areas

Governance: Develop a plan for how staff, business units, IT personnel and executives will protect sensitive information, critical resources and the organization’s reputation in light of the risks to these assets that a dynamic workforce poses.

Identity management: Choose methods of authentication and access control that provide a high level of assurance users are who they say they are, their access is in line with their responsibilities and what they are doing with that access is appropriate.

Data security: Take steps beyond identity management to further limit the risk to data posed by a dynamic workforce. Identify and secure sensitive data, determine where data is at the most risk and adopt appropriate policies, rules and controls to protect it.

Data privacy: Respect the individual right to keep personal information private, by complying with regulations, keeping employees and customers informed about data collection practices, and training employees and third parties in their responsibilities to protect data privacy.

System-level protections: Extend trust to endpoints—the various computers, phones, tablets and other network-enabled devices the workforce uses—by using endpoint detection and response (EDR) solutions to detect and respond to threats.

SECURE YOUR CLOUD TRANSFORMATION

Managing risk as you move operations to new technology architectures requires a comprehensive security and risk management approach.

Action Areas

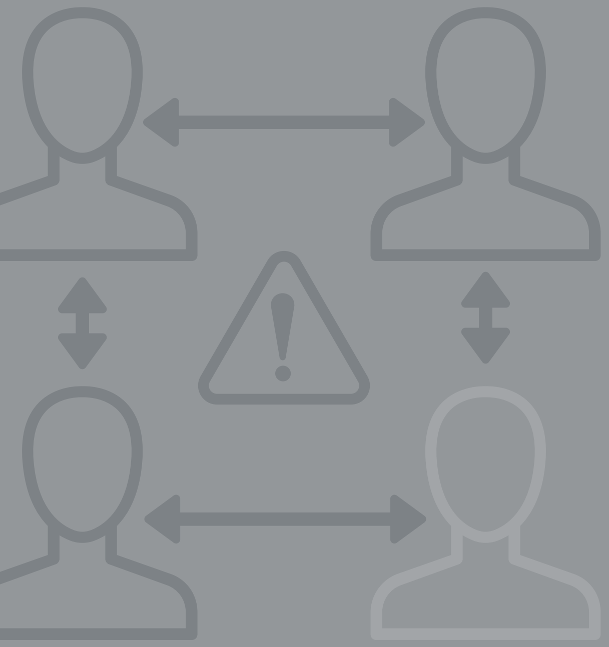
Ecosystem management: Identify and address potential vulnerabilities created by the complex ecosystem of hardware, software and third-party partners (including cloud providers, consultants, integrators and others) that supports cloud operations.

Governance: Establish policies and processes for managing relationships with cloud providers, including assessing their security capabilities and creating a RACI model to clarify who is ultimately responsible for which security issues and incidents.

Identity management: Go beyond basic identity controls to gain greater insight into authentication risk in the cloud, especially across multi-cloud environments. Consider risk-based authentication to increase security without overburdening users.

Compliance obligations: Implement compliance controls to meet regulatory demands in complex cloud environments, including data classification and location, continuous data-usage monitoring, evaluation of cloud providers' controls, and data privacy training.

MANAGE THIRD-PARTY RISK



Organizations using third parties to augment their own capabilities face the challenge to build, continually expand and safeguard a hyper-connected business ecosystem.

Action Areas

Ecosystem management: Establish ownership of, and define the criticality of, third-party relationships. This will make it easier for third-party engagements to proceed predictably and for issues to be resolved quickly.

Contracting: Clearly define the rules of engagement by always including scope, accountabilities and SLAs in contracts and legal agreements with third parties (and with the third parties' third parties, in some cases).

Identity management: Recognize the risk posed by third parties having access to the organization's sensitive information. Secure their access to critical resources and govern identities and access with an analytics-driven approach.

Governance: Use a programmatic, coordinated and risk-driven approach to manage third parties, including a comprehensive third-party governance program that focuses on three priorities—reducing risk, improving security and improving business performance.

HOW RSA CAN HELP

RSA has the people, technology, experience, partnerships and vision to help organizations manage the risks that stem from digital transformation. Our industry-leading solutions break down business and security silos so you can take control of digital risk.

GETTING STARTED

Begin with some simple, self-guided tools, like the RSA Digital Risk Index, which will help you understand your digital risk exposure and set priorities for different areas, and the RSA Cyber Incident Risk Framework Web Self-Assessment, which will help you assess your cyber incident risk posture.

Gauge your current risk management capabilities with the RSA Risk Frameworks, guided by the expertise of the RSA Risk & Cybersecurity Practice. The frameworks use industry guidelines and maturity models as the basis for detailed assessment of your strengths and weaknesses, and RSA experts provide prescriptive recommendations for how to mature digital risk management to support your business needs.

Explore the RSA products and services on the following page to learn more about how you can:

- Manage multiple dimensions of risk, across cloud, virtual and on-premises resources, from a single integrated platform.
- Orchestrate and automate threat response and other actions based on which threats pose the greatest risk to your business.
- Achieve a high level of confidence that users seeking access to resources are who they claim to be, with minimal user friction.
- Continuously govern access for both full-time and contract workers, as well as an expanding ecosystem of third-party vendors.
- Protect customers from fraud across web, mobile, ATM, call center (including IVR) and open-banking channels.

WORKING WITH RSA

Respond to risks proactively, with data-driven insights and a streamlined, fast time to value approach.

RSA ARCHER® SUITE

Rapidly detect and respond to any threat—on devices, in the cloud and across your virtual enterprise.

RSA NETWITNESS® PLATFORM

Provide your users with convenient, secure access to any application—from the cloud to the ground—from any device.

RSA SECURID® SUITE

Manage fraud and digital risks across multichannel environments without impacting customers or transactions.

RSA FRAUD & RISK INTELLIGENCE SUITE

Leverage strategic consulting services, staff augmentation and acute incident response services from RSA.

RSA RISK & CYBER SECURITY PRACTICE

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

[1] RSA Digital Risk Study, RSA Digital Risk Report—2nd Edition, January 2020, pp. 4-15

[2] Opinions expressed by Tony Arnold are his and do not necessarily reflect those of his organization.

RSA®

© 2020 Dell Inc. or its subsidiaries. All Rights Reserved. RSA and the RSA logo are trademarks of Dell Inc. or its subsidiaries in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. Published in the USA, 4/20 eBook W350909 H18216