RSA

MANAGING DIGITAL RISK

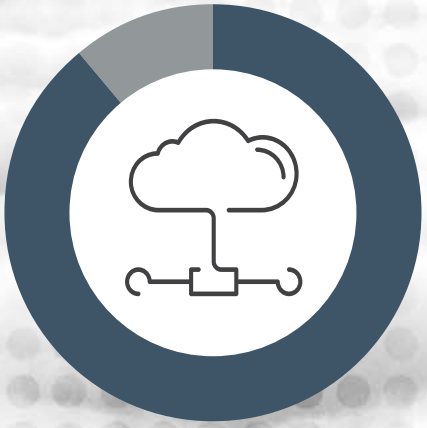
8 Types of Digital Risk and How to Manage Them

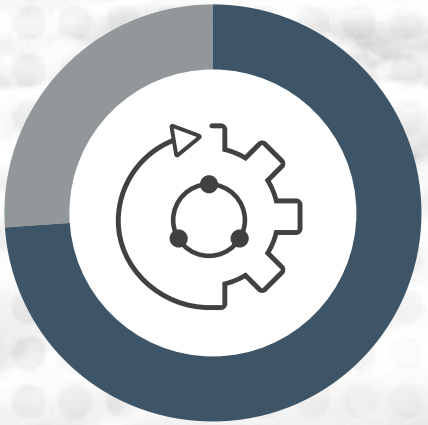
THE REALITY OF DIGITAL TRANSFORMATION

For many organizations, digital initiatives are a lifeline. Technologies such as IoT, social, machine learning, big data analytics, AI and augmented reality allow them to streamline operations, adopt new business models and improve the customer experience—maximizing speed, agility, efficiency and profitability.

89%

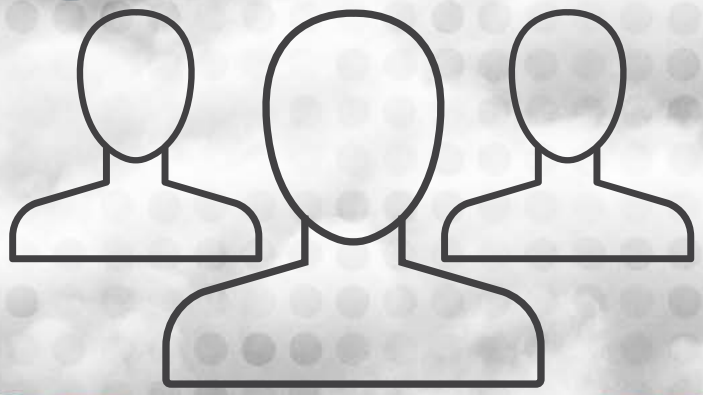
of organizations have adopted or have plans to adopt a digital-first strategy.[1]





74%

of executive decision makers see digital transformation as a priority.[2]

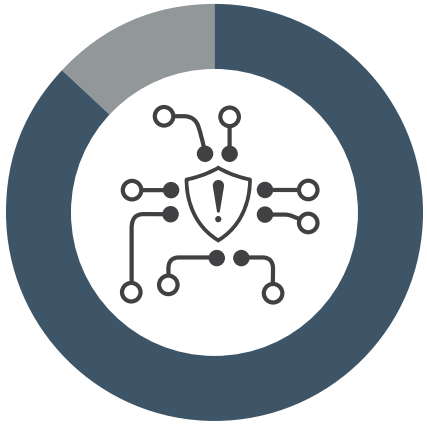


DIGITAL TRANSFORMATION AND DIGITAL RISK GO HAND IN HAND

What is digital risk?

Digital risk refers to unwanted—and often unexpected—outcomes stemming from digital transformation and the adoption of related technologies. Cybersecurity risk, third-party risk, business continuity risk, data privacy risk and other forms of digital risk add to the uncertainty of achieving business objectives.

Digital transformation creates tremendous business opportunities—along with new forms of digital risk.

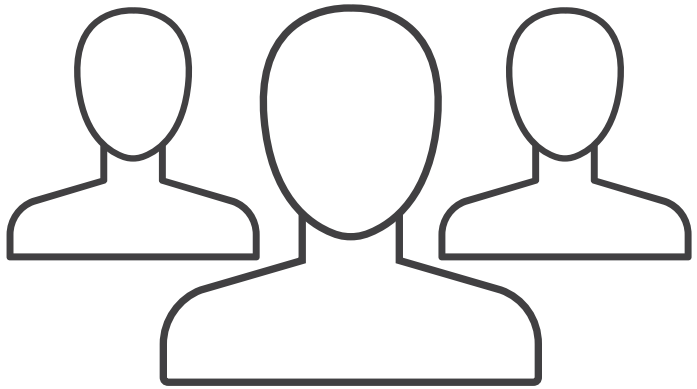


87%

of respondents report their risk profile has expanded somewhat or significantly due to new or increasing risks.[3]

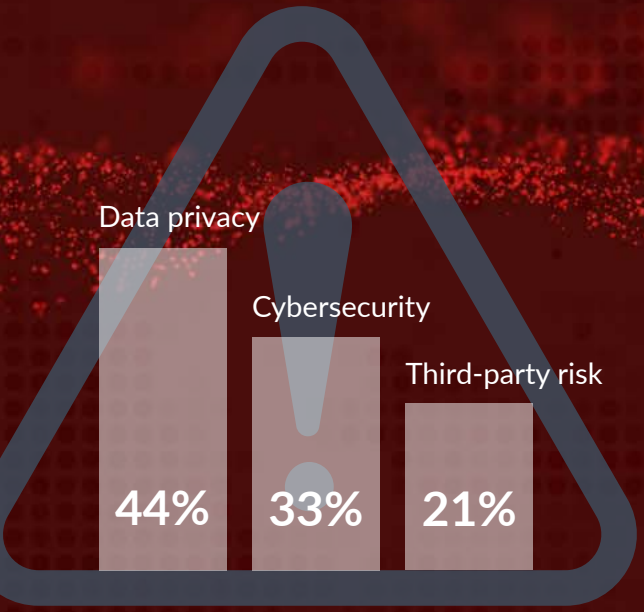
95%

of CEOs believe their organizations will face serious threats and disruption in the next three years.[4]



EIGHT TYPES OF DIGITAL RISK

Strategic business objectives—including new operational efficiencies, business models and customer experiences—are the driving force behind digital initiatives such as big data analytics, IoT and AI. But these initiatives have spawned eight types of digital risk that every organization must learn to manage.



Biggest Digital Risks

What is the biggest digital risk your organization currently faces?[5]

BUSINESS OBJECTIVES

- New Operational Efficiences
- New Business Models
- Improve Customer Service

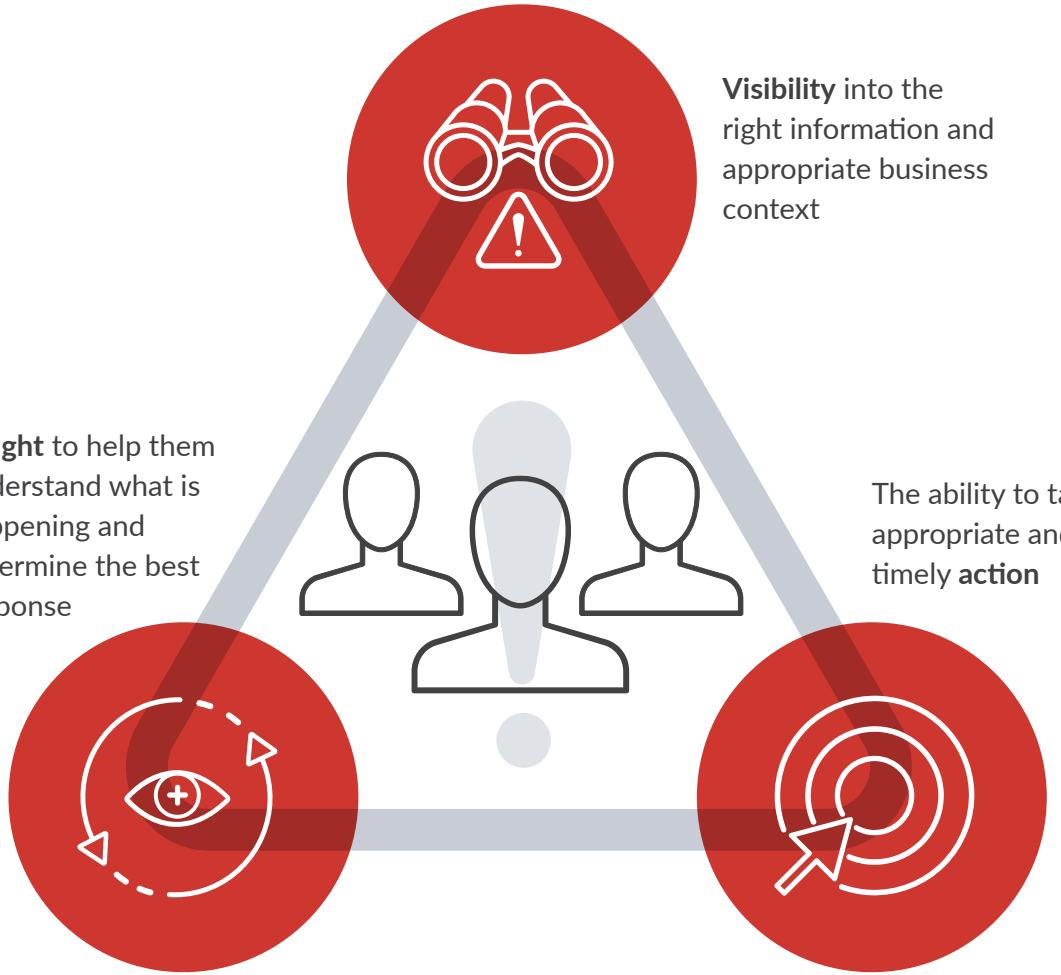
DIGITAL INITIATIVES

DIGITAL RISKS

CYBERSECURITY	Risk of cyber attacks, especially in the context of a growing attack surface and an increase in sophistication of attacks
WORKFORCE/ TALENT	Risk related to the dynamic nature of today's workforce and the gig economy
CLOUD	Risk due to changes in architecture, implementation, deployment and/or management of new digital business operations or IT systems
COMPLIANCE	Risks related to compliance requirements driven by new technology and the scope of data being created
THIRD-PARTY RISK	Inherited risk related to external parties
PROCESS AUTOMATION	Risk related to changes in processes from automation
RESILIENCY	Risk to availability of business operations, especially after disruption
DATA PRIVACY	Risks related to the ability to protect personal information

KEYS TO MANAGING DIGITAL RISK: VISIBILITY INSIGHT ACTION

To manage digital risk effectively, security and risk management teams must work together. When organizations align security and risk, they ensure:



Visibility into the right information and appropriate business context

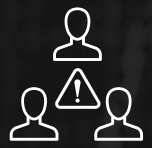
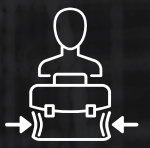
Insight to help them understand what is happening and determine the best response

The ability to take appropriate and timely **action**

GETTING STARTED WITH DIGITAL RISK MANAGEMENT

You know you need to focus on digital risk management, but where do you start? The question can be daunting, raising the possibility of initiatives that are overambitious, too disruptive or simply too long.

Don't panic. Start by targeting just one of the eight key risk areas and focusing your efforts there. As you progress, you'll develop strategies to help protect your organization while enabling innovation. Keep in mind that many of these risks have overlapping consequences, so putting a solution in place for one can help address others, too.

RISK AREA	 MITIGATE CYBER ATTACK RISK	 MANAGE THIRD-PARTY RISK	 MANAGE DYNAMIC WORKFORCE RISK	 SECURE YOUR CLOUD TRANSFORMATION	 MODERNIZE YOUR COMPLIANCE PROGRAM	 MANAGE PROCESS AUTOMATION RISK	 COORDINATE BUSINESS RESILIENCY	 EVOLVE DATA GOVERNANCE AND PRIVACY
FOCUS	Protect your digital business, customer information, brand and critical assets from cyber threats.	Build, continually expand and safeguard a hyper-connected business ecosystem.	Adapt to new digital paradigms for employee expectations, skills and needs.	Manage risk as you move operations to new technology architectures.	Meet today's regulatory challenges with an ongoing, programmatic approach.	As your digital and automation strategies unfold, ensure built-in risk evaluation.	Safeguard digital operations against a range of events.	Protect key information assets.

Let's review some examples of what managing risk looks like in organizations across a variety of industries.

GETTING STARTED WITH DIGITAL RISK MANAGEMENT

HEALTHCARE

Digital risk	Cyber Attack
Type of company	Regional health system that includes hospitals, physicians and pharmacies
Goal	Protect digital medical records and medical technology required to provide quality care from being compromised by a cyber attack.
Visibility and insight	Achieving the goal requires visibility into known and unknown threats to detect issues quickly and understand their impact on the healthcare system and patients. This includes being able to identify anomalous access activity to prevent unauthorized access to private patient data, and to understand the criticality and context of threats to prioritize responses effectively.
Action	Improve cyber attack mitigation by adopting evolved security capabilities integrating user behavior analysis, threat intelligence and risk-based identity and access management; develop a well-planned attack response process that extends from the security operations center (SOC) team to business leadership.
Result	An integrated approach to managing the risk of cyber attack improves the ability to detect and respond to threats in a well-orchestrated manner, minimizing the impact to health services, patient privacy, regulatory compliance and the organization's reputation and bottom line.

GETTING STARTED WITH DIGITAL RISK MANAGEMENT

BANKING

Digital Risk	Third-Party Risk
Type of Company	Regional bank operating dozens of branches across multiple geographic areas
Goal	Deliver secure omnichannel banking services through an extended ecosystem of business partners while managing the inherited risks of third-party relationships.
Visibility and insight	Achieving the goal requires visibility into third-party activity to effectively manage the potential risk of fraud, data breaches, noncompliance and other issues. This is especially critical in the API economy, in which banks open their systems to third parties to give customers the ability to link accounts with other services (utility payments, for example). Required in the EU by the PSD2 directive, this openness creates digital opportunity, but also increases third-party risk.
Action	Improve third-party governance by implementing an integrated risk management strategy designed to catalog, assess, evaluate, treat and monitor third-party risk, prioritizing areas where there is external access to internal systems and customer channels.
Result	An integrated approach improves third-party risk management by bringing together capabilities to track and monitor third-party activity, detect cyber threats in systems that third parties access, and authenticate third-party users and govern their access.

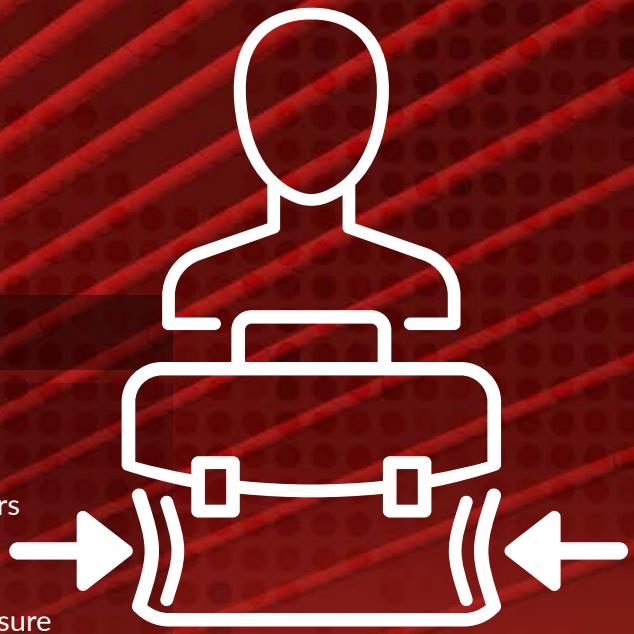
GETTING STARTED WITH DIGITAL RISK MANAGEMENT

ENERGY/RETAIL

Digital Risk	Dynamic Workforce
Type of Company	Oil and gas company operating a chain of retail gas stations
Goal	Manage the risk of inappropriate access that could lead to retail fraud or a data breach, while still providing frictionless access to a diverse workforce population.
Visibility and insight	Achieving the goal requires an integrated approach that provides complete visibility and insight into who users are, what they have access to and what they are doing with their access—along with the ability to uncover and respond quickly to issues.
Action	Roll out comprehensive capabilities to manage dynamic workforce risk, including risk-based multi-factor authentication, analytics to uncover access risks and violations, and user and entity behavior analytics (UEBA) to flag suspicious access behaviors.
Result	An integrated approach reduces risk by protecting at every point from initial authentication to access activity, in ways that expedite legitimate authentication and access by taking relative levels of risk into account.

GETTING STARTED WITH DIGITAL RISK MANAGEMENT

TRANSPORTATION SERVICES



Digital risk	Business Resiliency
Description	Airport operations
Mission	Provide a consistently safe, secure environment for millions of annual passengers and thousands of contractors, airline employees and other airport staff.
Visibility and insight	Achieving the goal requires comprehensive business continuity processes to ensure uninterrupted operations in the wake of a security incident or major event such as a cyber attack or natural disaster. In an increasingly digital world, this means having an integrated strategy for coordinating business resiliency that considers the interconnectedness of business and technology.
Action	Ensure optimal incident recovery by bringing business context to continuity and recovery planning and by implementing incident management and crisis management processes that enable access to integrated information from business and IT systems.
Result	An integrated approach to business resiliency improves incident response time by presenting all relevant data for action in one unified view.

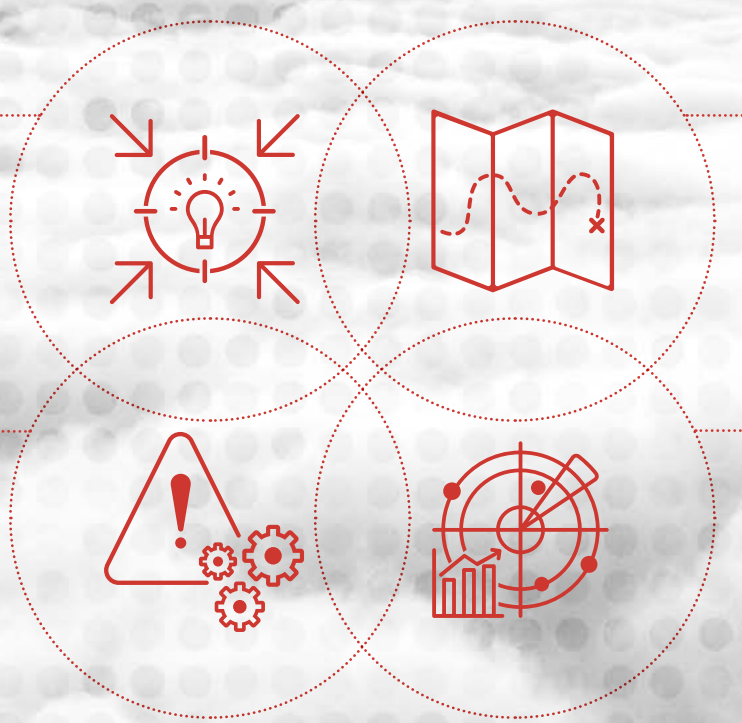
WHAT YOU NEED TO MANAGE DIGITAL RISK

A unified approach to managing digital risk hinges on integrated visibility, automated insights and coordinated actions.

With such an approach to digital risk, organizations can thrive in today's high-risk digital world.

Imagine:

Controlling risks associated with modern user and consumer access in today's connected world



Creating a tailored roadmap for **managing digital risk** as your organization matures

Protecting your digital future with a **unified approach to security and risk**

Being able to **quantify digital risk**

MANAGE DIGITAL RISK WITH BUSINESS-DRIVEN SECURITY

Risk management teams have traditionally operated in silos, focused on their own sliver of business risk. But digital risk is a concern that must be addressed across the enterprise—from the security operations center (SOC) to the boardroom; from front-line threat detectors to those making strategic decisions for the future.

RSA advocates a business-driven security approach in which risk management and IT teams are connected and security decisions are made based on business context. Business-driven security couples business risk information with data and intelligence from threat detection and response, identity management and fraud prevention systems, better equipping organizations to adapt to changing competitive pressures and confidently pursue digital opportunity.

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 2018 State of Digital Business Transformation, IDG Communications, April 2018

2 Digital Transformation: Strategies for Success, Salesforce, 2018

3 RSA, "Digital Risk Management: The Next Horizon of Risk" webinar poll, March 2019

4 CEO and Board Risk Management Survey, Deloitte, 2018

5 RSA, "Digital Risk Management: The Next Horizon of Risk" webinar poll, March 2019

RSA®