RSA

5 TIPS FOR MANAGING THIRD-PARTY RISK

YOUR THIRD PARTIES SHOULD ADD VALUE, NOT EXPOSURE

Digital Transformation & Third-Party Risk

Across industries and around the world, executives remain preoccupied with digital transformation. According to a 2018 survey of 500 business executives, 74 percent said digital transformation would be a priority for their organizations in the year ahead.[1]

Because digital transformation tends to be a large undertaking—frequently involving people, processes and technology across a company—organizations find they can't go it alone. They need partners. So digital transformation has the effect of increasing an organization's ecosystem of third-party partners.

These relationships can bring a host of benefits—organizations innovate and gain speed, efficiency and other capabilities from third parties—but they also add significant risk...

THIRD PARTIES CAN INTRODUCE **UNPREDICTABLE, INHERITED RISKS**

THIRD-PARTY RISKS ARE MORE COMPLEX AND INTERRELATED

Organizations face a myriad of risks arising from third parties, including data breaches, fraud and theft, business disruption, regulatory compliance violations, and reputational damage. These risks are often fast-moving, complex and interrelated, and because they're typically hidden within both your organization's activities and your third parties' activities, they can be hard to anticipate.

THIRD PARTIES ARE NOT MANAGED CONSISTENTLY

In many organizations, third-party relationships are managed in silos, across different business units or functions. Each function may have its own way of identifying, assessing and managing business partners. This not only leads to redundant activity; it also inhibits the executive management team's ability to get a complete and accurate view of third-party risk and performance across the organization. And without a firm grasp of their organization's third-party risk exposure, leadership can't make informed decisions about how much to invest—and where—to protect the business from these risks.

THIRD PARTIES ARE MORE CRITICAL TO ORGANIZATIONS

The more an organization depends on third parties to meet its business objectives, the more rigor it needs to apply to managing these relationships. Unfortunately, few organizations understand the extent of their dependence on third parties and the potential risks this dependence creates. As a result, they are unable to keep up with their organization's changing business landscape, challenges associated with their third parties, growth of third-party engagement, or their business's demand for agility.

1

KNOW YOUR THIRD PARTIES

A regulation in the financial services industry known as “Know Your Customer” requires financial institutions to verify the identity of their clients and assess potential risks. Ideally, organizations across all sectors should do the same with their external partners, since many organizations lack a clear understanding of their third-party dependencies.

Follow these steps to get started:

Catalog all third-party relationships and engagements, including the individuals responsible for each one.

Associate each third party with the business unit, division, function or business process that it supports.

Identify the system access or data access required for each third party and each of its agents to carry out their contractual obligations.

Determine which performance metrics to track during the course of a third party’s engagement with your company.

2

UNDERSTAND THEIR IMPACT

A typical organization may use hundreds, if not thousands, of third parties. These partners will require varying levels of due diligence and oversight depending on the importance of the products, services or capabilities they provide. The more critical the third party, the more rigorous governance the partner is likely to require.

To understand the nature and scope of your organization's dependence on its third parties, heed the following advice:

Leverage existing business impact analysis studies to determine the criticality of each area of the business and tie that criticality to the third parties supporting each area.

Identify and evaluate risks to determine the level of exposure each third party (and their products or services) poses to the organization.

Assign the appropriate levels of system access to third parties and their agents based on their responsibilities and risk to the organization.

Adjust third-party governance, assessment and monitoring activities based on each partners' criticality to the business.

3

EVALUATE YOUR THIRD-PARTY RISKS & TAKE ACTION

Many third-party relationships introduce unpredictable, inherited risks that result in losses to an organization. Since it's not possible to transfer all risks to third parties through contractual agreements, a risk management process based on standards and best practices can help your organization identify, assess, treat and monitor these risks. A standards-based risk management process can also ensure that:

- Stakeholders across the enterprise make decisions about third-party risks consistently and in accordance with the organization's risk appetite;
- The executive management team understands third-party risk exposure in its entirety, enabling them to determine how much to invest to protect their business from these risks;
- Regulators requiring rigorous oversight of third-party relationships understand an acceptable risk management approach is in place.

A sound risk management process should encompass the following activities:

Assessing and managing requests from business line managers to initiate new third-party relationships.

Documenting third-party relationships and associated contracts, and establishing business owners within the organization who are responsible for each relationship.

Conducting risk assessments of each third party's control environment; leveraging the assessment results to determine the vendor's residual risk across applicable risk categories; and taking appropriate action to reduce risk to acceptable levels.

Documenting and monitoring performance and service-level metrics for each vendor and each product or service they offer.

4

MONITOR YOUR THIRD PARTIES

Effective third-party management doesn't stop once partners are on board and working—in fact, that's just the beginning. Many aspects of third-party relationships can, and usually do, change. For instance, third parties may introduce new risks. Their financial situations may shift, and their employees may come and go, necessitating access changes. Therefore, it's vital to have the right processes and metrics in place to monitor third parties, their access to your systems and data, and their overall ability to support your business objectives.

Proper oversight should include:

- Documenting performance and service-level metrics for each third-party product and service, and monitoring that each engagement is being delivered in accordance with expected outcomes.
- Monitoring the online access of each third party, their employees and fourth parties, and assessing and responding to risk, compliance and security issues related to third-party access.
- Implementing real-time threat detection and response capabilities to identify fraud attempts and other malicious activities originating from third parties.
- Adjusting your monitoring activities so that your most critical third parties get the most scrutiny.

5

COORDINATE SECURITY, RISK & BUSINESS TEAMS

Because third parties can introduce such a wide range of risks, managing third-party risk and performance in the age of digital transformation requires close collaboration among security, risk and business functions. Together, these teams can ensure that decisions about third-party risks are made consistently across the business, and that risk and security considerations are front and center when new third parties are being assessed and evaluated. Third-party viability, criticality, performance, risk and security must be coordinated together throughout the third-party governance lifecycle.

RSA HELPS YOU MANAGE THIRD-PARTY RISK

RSA® Business-Driven Security™ solutions provide a coordinated, programmatic approach to managing third-party risk across IT, security, risk management, fraud and business functions. While other vendors may provide individual capabilities for managing third parties, our tightly integrated products and advisory services can help you gain control of the full spectrum of risks emanating from these partners while improving governance, efficiency and performance.

HOW WE HELP

ASSESS THIRD-PARTY RISK-MANAGEMENT CAPABILITIES

- Engagement
- Assessment
- Risk Quantification Model
- Benchmark Report

RSA® RISK & CYBER SECURITY PRACTICE

EVOLVED SIEM/ ADVANCED THREAT DETECTION & RESPONSE

- Security Platform
- Logs & Packets
- Endpoint
- UEBA
- Orchestration & Automation

RSA NETWITNESS® PLATFORM

THIRD-PARTY GOVERNANCE

- Business Context
- Criticality & Priority
- Risk Assessment
- Monitoring
- Dashboards & Reporting

RSA ARCHER® SUITE

SECURE, RISK-BASED ACCESS & AUTHENTICATION

- Risk-Based Authentication
- Authentication Anomaly Detection
- Identity, Governance & Lifecycle Management
- Access Policy Violation Detection

RSA SECURID® SUITE

OMNI-CHANNEL FRAUD PREVENTION

- Omni-Channel Fraud Detection
- Advanced Adaptive Authentication
- Real Time Risk Assessment
- Fraud Intelligence

RSA® FRAUD & RISK INTELLIGENCE SUITE

Review some resources that will help you take the first step toward strengthening your organization's third-party risk posture:
rsa.com/en-us/products/integrated-risk-management/third-party-governance

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. Salesforce.com, "Digital Transformation: Strategies for Success," p.2 https://www.salesforce.com/blog/2018/07/customer-success-digital-transformation-north-star-report.html (July 2018).