MANAGE THIRD-PARTY RISK

ASSESS NEW RISKS AS YOUR THIRD-PARTY ECOSYSTEM GROWS

DIGITAL TRANSFORMATION LEADS TO EXPANSION OF THIRD-PARTY ECOSYSTEMS

Digital transformation is making many organizations increasingly reliant on third parties. In a Deloitte poll of more than 4,000 finance and risk management professionals, 70 percent of respondents reported a moderate to high level of dependence on external entities, including third-, fourth- and fifth parties.[1] Deloitte also found that the number of third parties that organizations use increased 15 percent from 2017 to 2018.[2]

Figure 1: Growth of Third-Party Risk, Source: RSA

The growth of third-party ecosystems means organizations are gaining access to the critical capabilities they need to grow and compete more effectively. But as these digitally connected ecosystems grow, so too do the risks. Nearly half (47 percent) of respondents to the Deloitte poll said their organizations experienced some sort of risk incident in the last three years as a result of using external entities. These negative events suggest that traditional risk management methods are not detecting or mitigating the risks well enough. This may be a result of organizations not scaling their risk management process adequately to meet the growth of third-party ecosystems and third-party management requiring more efficient and risk-based governance than traditional methods can provide.

GAPS IN THIRD-PARTY GOVERNANCE PROGRAMS

Many organizations' third-party governance programs have gaps that stem from the following issues:

According to the 2018 Cost of Data Breach Study by the Ponemon Institute, factors that increase the cost of a data breach include: **third party involvement**, extensive cloud migration, compliance failure, and the extensive use of mobile platforms.[3]

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. As if those issues weren't enough, a third party's poor performance could compromise an organization's ability to meet its strategic objectives. These risks are often fast moving, complex and interrelated. For example, if a third-party technology provider experiences a data breach, the breach may affect client data. What's more, the business disruption caused by the breach may result in service outages for clients, and those service outages could create an uproar on social media leading to lost customers, lost revenue and lasting reputational damage. Because these risks typically stem from the third parties' activities or inadequate risk management on their part, they often come as a complete surprise.

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 third parties. This not only leads to redundant activity; it also inhibits the use of best practices across the organization. Further, the executive management team is unable to get a complete and accurate view of third-party risk and performance across the organization. And without a firm grasp of their entire 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 becoming 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 implement the appropriate measures to manage their existing third parties and address challenges resulting from a constantly changing third-party landscape—all while meeting their business's demand for agility.

In short, managing third-party risk in the age of digital transformation requires a programmatic approach that's part of a truly integrated risk management strategy. A comprehensive third-party governance program should focus on understanding and managing risks while improving business performance.

> *"A lot of organizations have suffered breaches through third-party risks in the last couple of years, so we want to make sure we're using RSA tools to help monitor third-party use of our system and make sure we aren't vulnerable."*
>
> Rich Rogers
> Senior Vice President & CIO
> **Prisma Health (formerly Greenville Health System)**

HOW RSA CAN HELP

RSA approaches third-party governance from several coordinated perspectives to give you the visibility, insights and actions you need to optimally manage third-party risk. RSA can help you:

- Evaluate your overall third-party governance capabilities and identify areas for improvement.
- Establish the business context necessary to understand how and where third parties are used and their importance to your organization.

- Implement a programmatic approach to identify, catalog, assess, evaluate, treat and monitor third-party risk, including risks associated with your third parties' employees and their activities.
- Determine the level of risk each third-party product and service poses to your organization and understand which third parties pose the most risk.
- Evaluate the adequacy of third-party risk treatments and monitor remediation of any identified deficiencies.
- Manage third parties' access to your internal systems, data and consumer-facing systems to ensure they don't have excess access.
- Monitor your entire IT environment so that you can rapidly detect and respond to information security and fraud threats introduced by external entities.

The RSA solution for third-party risk management helps you mature, automate and streamline oversight of your external relationships, enabling you to better understand, prioritize and manage the entire third-party lifecycle. RSA is the only third-party risk management solution that brings together the following products to help you manage business, information security and fraud risk related to your extended ecosystem.

RSA Archer® Suite: Track each third party and their activities so you understand the criticality and risk of each in the context of your business. Assess the governance and controls that third parties have in place around the products and services they are delivering to your organization, and understand any residual risk and deficiencies that must be remediated. Monitor each third party's performance by establishing metrics for each engagement and relationship.

RSA NetWitness® Platform: Monitor and respond to risk, compliance, information security issues and fraud attempts by collecting data across capture points and computing platforms utilized by third parties. Speed threat detection, investigation and mitigation by enriching log, network and endpoint data at capture time with threat intelligence and business context. Automate and orchestrate incident response to reduce the risk of security breaches and fraud attempts originating from third parties.

RSA SecurID® Suite: Protect critical internal systems, sensitive data and your consumer-facing digital channels by better governing third-party access with a risk-based, automated approach that certifies identities, assigns appropriate levels of access based on users' responsibilities, and scales to meet the unique demands of authenticating third-party users.

RSA® Fraud & Risk Intelligence Suite: Detect, monitor and respond to third party-related fraud threats in your consumer-facing digital channels with a combination of actionable fraud intelligence, real-time behavioral analytics and risk-based adaptive authentication.

RSA® Third-Party Risk Framework: Assess your organization's third-party governance capabilities and get a detailed roadmap tailored to your business.

YOUR TRUSTED PARTNER FOR THIRD-PARTY RISK

Nearly half of CEOs and board members surveyed by Deloitte say they're planning to either develop new or improve existing programs for managing third-party risk. They're also planning to invest in new technology to automate assessment and monitoring of third-party risks.[4] As your organization leverages third parties to execute its business strategy, consider RSA to help you on this journey. The RSA solution for managing third-party risk offers a coordinated, programmatic approach 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.

ABOUT RSA

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection and integrated risk management, RSA customers can thrive and continuously adapt to transformational change. For more information, go to rsa.com.

1. Deloitte, "Reestablishing the Perimeter: Extending the risk management ecosystem" (October 2018)
2. Tom Fox, "Managing the Extended Enterprise: A Conversation with Tom Kinsella," Innovation in Compliance Podcast (February 26, 2019)
3. Ponemon Institute, "2018 Cost of a Data Breach Study" (July 2018)
4. Deloitte, "CEO and board risk management survey: Illuminating a path forward on strategic risk" (2018)