Deloitte.

The rising importance of third party risk management (TPRM)

October 2024

Introduction

Business has rapidly changed over the last few years, with organizations expediting their digital strategies to meet the changing needs of a post-pandemic world. Today 60% of the organizations are dependent on working with over 1,000 third parties[1], and these numbers will only continue to increase as business ecosystems expand and become more complex.

> 60% of organizations are now working with more than 1,000 third parties.

With greater reliance on third parties and a broader supply chain to support services comes greater risk of operational disruption. At the same time, threats are becoming increasingly sophisticated, driving greater risk across the third-party ecosystem that can have lasting damage on customer trust in the event of a data breach.

Organizations need to find ways to manage third party risks at scale, drive efficiency, and minimize exposures while enabling business outcomes.

While it is exciting to imagine the business potential of outsourcing services, it also brings an urgency to rethink how third party risk exposures are identified and managed. The traditional approaches for evaluating third party risk have not kept pace with the growth and complexity of today's globally connected business environment and accompanying risk exposures. As a result, organizations are unable to effectively assess and evaluate risk within the third party ecosystem.

Without proactive and continuous monitoring of third party risks, organizations become increasingly vulnerable to risks such as supply chain disruption, reputational damage, and cyber breaches. Organizations need to transform their TPRM processes by balancing traditional risk management methods with the adoption of next-generation services and capabilities.

Emerging risks across the third party ecosystem—Why should you care?

Across industries, many organizations focus on cyber, information security, and privacy-related risks due to regulatory or compliance mandates as well as the potential impact and costs associated with information-related breaches. In fact, the average total cost of a data breach in the United States was $9.44M in 2022[2]. Of course, not all data breach incidents are third-party or supply chain-related—however, a recent study found 19% of breaches occurred because of a compromise at a business partner or third party. Ransomware and destructive attacks were responsible for more than a quarter of breaches in critical infrastructure industries. Of those breaches, supply chain attacks where a third party business ecosystem partner was the attack vector, accounted for 17%.[3]

Taking a step outside of data privacy and cyber security, TPRM programs with greater maturity also evaluate broader risk domains with potentially significant risk exposures, such as operational resilience, reputation risk, and financial viability.

To help you consider which risks are pertinent to your organization, below is a list of commonly evaluated risk domains that span the third-party ecosystem:

Cyber/information security

Exposure created from a third party's use, storage, and communication of information that is vulnerable to accidental or malicious alteration, destru ction, or unauthorized access

Resiliency

Failure to supply goods or services due to inadequate management of a disruptive event (e.g., operational disruptions, natural disasters, pandemics, climate change), resulting in adverse impact

Geographic

Exposures resulting from a third party's physical geographic location of operations, data center, or digital assets

Concentration

Excessive dependence on a single third or fourth party for the provision of goods or services. Exposure may also arise from geographic concentration of third-party services.

Health & Safety

Delivery of goods or services in a manner that contributes to a fatality and/or causes harm to employees or other contractors/third parties.

Anti-bribery and corruption

Exposure to a third party engaging in unlawful business practices or criminal behavior, such as money laundering, bribery, or fraud.

Environmental, Social & Governance (ESG)

Engagement in activities that adversely impact people (e.g., modern slavery, labor rights) or the environment (e.g., carbon emissions, land protection) without regard for remediation or mitigation

Compliance

Non-compliance with laws, regulations, or ethical standards, including conflict of interest, resulting in censure from regulators, litigations, and/or other adverse impacts

Nth-tier suppliers

Risk exposure created by hidden or unknown external suppliers or vendors beyond the direct third-party relationship

Reputation

Brand and marketplace risk exposures to reputation created by a third-party supplier or vendor's actions, statements, and business dealings—including working with poorly managed or unfair business partners, which can affect the public's perception and brand equity of your organization

Financial viability

Exposure to a third party becoming financially nonviable and therefore unable to deliver a stable service or product

Conduct

Exposures related to general misconduct that occurs within an organization, often seen as a circumstance of company culture, specifically related to sales and trading business practices

The business case for change in TPRM

As discussed above, the dependence on third party services continues to expand, and along with it, the risk to your organization. Accordingly, organizations should reevaluate the way they manage third-party risk.

Below are the major cross-industry business drivers and trends propelling the evolution of traditional TPRM solutions.

Regulatory pressure & senior executive expectations

Due to recent pervasive disruptions and major data breaches, there is increasing regulatory attention and action related to management of third-party risks and supply chain resilience. To confirm programs can appropriately meet changing regulatory requirements and industry expectations, TPRM programs are receiving exposure at the highest executive levels.

Growing threat landscape

Threats are becoming increasingly sophisticated, driving greater risk across the third-party ecosystem that can have lasting damage on customer trust in the event of a data breach. Furthermore, 2022's losses from data breaches cost victims $1.2 billion, an 80% increase over 2021[4]. These threats require dynamic risk management capabilities to match their accelerating growth and complexity.

Operational resilience

With greater dependance on third parties and a broader supply chain to support essential services comes greater risk of operational disruption. The COVID-19 pandemic exposed just how fragile supply chains are for many organizations. To increase operational resilience and minimize disruptions, organizations should proactively identify and illuminate hidden and unforeseen risks across their ecosystem of suppliers and vendors.

Need for business enablement

Many organizations struggle with a 'check-the-box' approach to third-party risk management that results in the overuse of static assessments—and the resulting assessment fatigue. In addition, these static assessments reduce business efficiencies, resulting in additional delays and cost overruns. With a growing ecosystem of suppliers and vendors, this approach may be neither scalable nor effective for many organizations.

Challenges with the traditional TPRM approach

The traditional TPRM approach does not align with the hidden risk and unforeseen vulnerability many organizations face today. The static and manual processes of many traditional TPRM approaches can require many resources but lack measurable risk-management value.

Below are some of the current challenges associated with traditional TPRM processes.

Point-in-time assessments

Traditional point-in-time TPRM assessments are usually manually intensive, low-value "check the box" compliance exercises used to measure third party control exposures. The static nature of point-in-time controls assessments limits the ability to continuously manage risk. Once the assessments are conducted, the assessment data typically becomes stale and underutilized.

Ever-growing Nth Tier ecosystem introduce emerging threats

Organizations can become deluged with their growing Nth Tier ecosystem of suppliers and vendors. These Nth Tier ecosystem relationships can introduce unforeseen threats. To help assess and manage emerging third party threats, some organizations use internal risk evaluation tools or utilize risk rating providers.

However, by relying on disparate data sources without proper correlation and analysis, organizations can overlook or miss emerging risks and threats.

Fragmented technology

Most organizations do not have a comprehensive view their extended integrated technology and data ecosystem. Without a centralized technology and risk assessment workflow, it becomes increasingly difficult and inefficient to manage growing third-party relationships and associated risks.

Talent and knowledge siloes

Not only are technology and data utilized in siloes, the risk domain/third party risk knowledge, processes, and strategy are spread across the organization, resulting in a lack of cross-functional collaboration. Additionally, talent and skillsets are typically compliance/assessment-focused, which is useful but may need to be complemented with more proactive risk-management skills.

Supply chain blind spots

Some organizations leverage contractual agreements to identify usage of fourth- and fifth-party suppliers, but these relationships are often unlinked to the third party's risk profile. For many organizations, there is limited visibility into relationships beyond the direct third party, meaning the business does not understand the subservice dependencies and associated risks, including geographic and supplier-specific concentrations within its supply chain. Similarly, there is little to no insight into software composition when considering the software supply chain.

Legacy third-party access to systems

For certain third-party relationships, network access and connectivity are crucial to the service provided. However, the use of outdated technology to grant and control third-party access to systems and networks can lead to a potential susceptibility to unauthorized access.

Think about it this way: If a third party contractor who has access to your IT environment experiences a cyber-attack, what is stopping the adversary from also infiltrating your own environment?

Innovation opportunities within TPRM—finding the balance between traditional and next-generation solutions

Effective TPRM programs find a balance between traditional point-in-time and next-gen continuous monitoring methods by taking a risk-based approach to application of capabilities that enables increased breadth of risk insight across the third party ecosystem and depth in the most critical areas. Below are innovation opportunities that address many traditional TPRM solutions.

Continuous monitoring

This involves an ongoing management of risks and threats throughout the third party ecosystem as opposed to solely conducting a cadence-based controls assessments. The application of continuous monitoring insights enables a risk-based approach to TPRM, leading to a potential reduction of traditional assessment volume, intelligently enhanced assessment scoping processes, and quicker risk takedown on an ongoing basis.

Risk and threat intelligence

Gathering meaningful and diverse cross-risk and threat-intelligence data can provide a holistic view of third-party risks. The application of correlation, analytics, and impact analysis then enables actionable insights and faster response to prioritized risks, threats, and events.

Single pane of glass and operations center

Leveraging standardized dashboards with correlated and aggregated information / data across the third party ecosystem entities enable operational and risk analysts to quick identify, triage, and initiate response activities.

Supply chain transparency

Incorporating illumination and software supply-chain analysis capabilities will identify fourth- and fifth-party supplier networks and uncover risky software vulnerabilities, help prioritize issues within the supply chain network, and more effectively scope inherent risk of direct third party providers.

Next-gen talent model

Discovering third party risk specialists and broader risk-management practitioners is crucial. Developing and investing in the next-generation talent is essential for organizations to build strategic and technical risk-response skillsets.

Secure access and anomaly detection

The next-generation TPRM solution integrates network security from a supplier and vendor point of view. If your extended ecosystem of third parties' suppliers and vendors require access to your organization's network, then your risk exponentially grows. Secure Access Service Edge (SASE) capabilities enable web-based granular access control and authentication, while Artificial Intelligence/ Machine Learning (AI/ML) detect anomalies in user behavior, data usage, system access, and insecure connectivity.

So, where do you go from here?

Well, you shouldn't feel like your organization has to take on this transformation on its own. Ongoing conversations with clients, and experience from engagements, indicate that effective TPRM programs increasingly depend on external assistance from trusted advisors. That's not only true for transformation projects (including design and implementation) but also for certain aspects of day-to-day execution of TPRM activities.

The 2022 Deloitte global third-party risk management survey found that organizations are complementing their in-house TPRM capabilities with external assistance[5]. This means they gain faster, more efficient access to readily trained resources and next-generation technology.

Managed service providers can both expedite the transformation process and provide day-to-day execution of TPRM activities.

Deloitte's perspective on a TPRM managed service

Managed service solutions are here to stay. While it is true that building talent and technology capabilities in-house can sometimes provide cost advantages, the problem is that in-house programs can limit speed and agility— including the ability to rapidly respond to regulatory shifts while addressing emerging skill, resources, and/or ecosystem needs.

The common challenges to developing in-house TPRM managed services talent and technology capabilities include:

- Lack of understanding of new risk threats, events, and disruptive technologies
- Lengthy adjustments to shifts in market trends and regulatory requirements
- Legacy technologies and systems are often out of date
- Existing approaches are not responsive, service-oriented, or adaptive to business needs

Our survey shows that managed service solutions from more established TPRM managed providers enable organizations to take advantage of disruptive solutions that challenge traditional approaches. The disruptive solutions include cloud, robotics process automation (RPA), and artificial intelligence (AI).

When executed well, managed service providers deliver measurable competitive advantages by transforming the way an organization operates. This leads to improved organizational performance, speed to market, and innovation.

Today, organizations are transitioning to more dynamic business models and increasingly flexible organizational structures, while attempting to reduce their capital expenditures.

As part of the transition to take advantage of dynamic business models, organizations are rapidly replacing traditional fixed-term, fixed-scope affiliations with more flexible managed-services relationships and platforms.

New engagement models

At the same time, the ever-changing business environment demands refreshed priorities and new engagement models.

While some organizations continue to focus on cost reduction, other organizations are transitioning to self-funding models. The return on investment achieved from TPRM services relationships are frequently directed to business transformation, the creation of new revenue sources, or customer acquisition.

And this transformation is happening at a time when market competition and new entrants are raising the stakes. Despite these challenges, TPRM services can provide an opportunity to benefit from real-time decision making while leveraging diverse yet interconnected analytical insights.

Outsourcing TPRM services can provide attractive propositions for organizations seeking to continually enhance their competitive advantage.

The benefits of next-gen monitoring in TPRM programs

Actionable insights

Advanced analytics and event data logs provide actionable ecosystem risk insights and analysis

Alert creation and resource management

Detection of emerging threats or changes in the ecosystem risk profile triggers alerts for subject-matter specialists to triage and conduct risk analysis.

Ecosystem risk profile

Intuitive dashboards and reports provide full view of the partner and vendor supplier risk profile

Risk analysis

Deloitte subject-matter specialists perform targeted risk investigation that leverage available data source and ecosystem profile characteris

Continuous risk monitoring

Advanced correlation capabilities continuously sense and monitor asymmetric risk across internal and external data sources.

Remediation

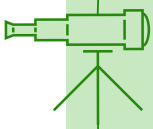
Customized triage playbooks enable proactive remediation. Bring human insight and technology into balance to proactively monitor and respond to ecosystem risk while preparing for evolving threats

Extended Tier N Illumination

Gain a broad view of both known and hdden Extended Tier N supplier, vendors and partners. Identify and expose unknown vulnerabilities to supply chain risk and disruption

Ongoing opportunities

The next-generation solution incorporates artifical intelligence and machine learning to enhance risk monitoring, detection and response capabilities.



Looking forward

Third party risk management continues to play an integral role in safeguarding privacy, safety, and trust within the supply chain. As times evolve and the world becomes increasingly interconnected, TPRM processes and procedures will need to continuously adapt. Organizations on the leading edge of this transformation are currently realizing the benefits, while organizations who lag or resist the change may become stuck in their old ways—until an adverse third-party event occurs.

As a business community, let's drive toward proactive risk management to help our people and organizations thrive in a more trustworthy, resilient, and secure environment.

To learn more about next-generation TPRM, don't hesitate to contact us.

Endnotes

1. https://apexassembly.com/third-party-risk-management-is-your-organization-reaping-the-rewards-or-simply-ticking-a-box/ Deloitte internal sources.
2. Ponemon Institute: Cost of a Data Breach Report 2022
3. ForgeRock: Consumer Identity Breach Report 2022.
4. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
5. Deloitte: Global third-party risk management survey 2022

Contact us:

Daniel Soo
Principal
Cyber Risk Services
Deloitte & Touche LLP
dsoo@deloitte.com

Suzanne Denton
Managing Director
Third Party Risk Management Leader
Deloitte & Touche LLP
sudenton@deloitte.com

Walter Hoogmoed
Principal
Third Party Risk Management Leader
Deloitte & Touche LLP
whoogmoed@deloitte.com

Samuel Icasiano
Managing Director
Cyber and Strategic Risk Leader
Deloitte & Touche LLP
saicasiano@deloitte.com

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Please see www.deloitte.com/about to learn more about our global network of member firms.