TPRM (Third-Party Risk Management) Cyber/IT Challenges

Today, over 60% of data breaches are traceable to third-party vendors. While engaging with third-party vendors is essential for business growth and operational flexibility, it also comes with potential risks that must be carefully managed to protect sensitive information. Given the interconnected nature of modern business operations, ongoing monitoring of third parties' security practices is critical to your organization's data integrity.

The 12 most common third-party risk management (TRPM) challenges with solutions to address them:

1 Cybersecurity Concerns

THE CHALLENGE: Third-party vendors' weak security practices, such as outdated systems, inadequate access controls, and insufficient incident response planning, could expose your sensitive data.

THE SOLUTION: Emphasize continuous monitoring of your vendors' security posture, including threat intelligence feeds and vulnerability scanning. Conduct regular simulated incident response drills with key vendors to test preparedness.

2 Regulatory Compliance

THE CHALLENGE: Failure to ensure third-party compliance with rapidly evolving regulations (e.g., GDPR, CCPA, industry-specific) can lead to significant legal and financial penalties.

THE SOLUTION: Stay informed about relevant regulations and industry standards. Regularly review and update third-party contracts to ensure compliance with regulatory requirements. If that proves too labor-intensive, enlist the help of a dedicated team, or consider software specifically for regulatory compliance tracking.

3 Data Privacy in the Cloud

THE CHALLENGE: Increased reliance on cloud-based vendors where data storage and processing occur outside of your direct control creates complexities in ensuring data privacy and adherence to regulations.

THE SOLUTION: Encrypt sensitive data in transit and at rest. Conduct thorough due diligence on cloud providers' security practices and establish data handling protocols and access controls within contracts.

4 Contractual Vulnerabilities

THE CHALLENGE: Vendor contracts that lack clearly defined cybersecurity expectations, responsibilities, breach protocols, and consequences leave your organization liable and exposed in the event of an incident.

THE SOLUTION: Strengthen contracts by explicitly outlining cybersecurity responsibilities, incident response procedures, and potential penalties for non-compliance. Include regular cybersecurity health checks and the right to conduct audits of critical vendors.

5 Lack of Visibility

THE CHALLENGE: The more vendors, suppliers, and partners that comprise your third-party ecosystem, the harder it becomes to track and monitor their activities. To make matters worse, when data is fragmented across departments like accounting, procurement, legal, and IT, it becomes even harder to gain a comprehensive understanding of the entire third-party landscape, potentially leaving critical risks undetected and unmanaged.

THE SOLUTION: Integrate a unified vendor data platform with existing IT systems for a cohesive view. This integration promotes efficient data sharing and analysis across various departments, such as accounting, procurement, legal, and IT, ensuring no critical risks are missed. Automated tools should be employed for scalable, continuous monitoring of vendors' cybersecurity health. Regular audits are necessary to identify and address vulnerabilities within the third-party ecosystem.

6 Multi-Layered Third-Party Relationships

THE CHALLENGE: Managing subcontractors and the extended networks of your third-party vendors introduces hidden risks to your supply chain. The limited visibility and control over these fourth-party networks can lead to a range of issues that are often difficult to anticipate and mitigate.

THE SOLUTION: Consolidate vendor relationships where possible. Establish clear guidelines for subcontracting and mandate visibility into those relationships. Rank vendors by how critical they are to your operations and tailor your risk management protocols to match. Use a centralized TPRM platform that facilitates vendor onboarding, automates risk assessment, and allows for continuous oversight. This platform should incorporate real-time threat intelligence and standardized questionnaires grounded in industry best practices to simplify the risk evaluation process and keep pace with emerging threats.

7 Inconsistent Standards and Practices

THE CHALLENGE: The lack of consistent cybersecurity standards, frameworks, and assessment methodologies across your third-party ecosystem makes it difficult to benchmark, compare, and effectively manage risk. Additionally, disparate security practices can introduce vulnerabilities and create blind spots within your larger risk posture.

THE SOLUTION: Promote the adoption of industry-recognized standards like the NIST Cybersecurity Framework or ISO 27001 across your vendor network to streamline assessments and create a common baseline for vendor security. Conduct tailored risk assessments based on the criticality of the vendor and the specific services they provide for a more focused approach and optimum resource allocation. Actively collaborate with third parties to elevate their security practices and alignment with your established standards. Provide resources and support where needed, especially for smaller vendors that may lack the expertise or means to meet your standards independently.

8 Dependency Risks

THE CHALLENGE: Overreliance on a few critical third-party vendors can leave your business vulnerable to significant disruption in the event of their failure or a security breach.

THE SOLUTION: Diversify vendor relationships and continuously analyze the market for alternative vendors and solutions. Develop contingency plans for reduced dependency risks, and conduct regular cybersecurity awareness training for all employees, focusing on the unique risks presented by third-party relationships.

9 Resource Constraints

THE CHALLENGE: Managing third parties becomes more difficult when resources are scarce in terms of time, budgets, and skilled personnel. The growing struggle to attract and retain talent skilled in cybersecurity and vendor management only exacerbates the issue, which can lead to gaps in cybersecurity protection and response.

THE SOLUTION: Provide specialized TPRM training programs for your procurement and vendor management team members and consider collaborating with cybersecurity experts to extend your teams' expertise even further. Implement technology that automates routine tasks so your team can focus their efforts on the more complex risk assessment activities.

10 Vendor Fatigue

THE CHALLENGE: Third-party vendors are bombarded with security questionnaires, which can lead to response fatigue and potentially inaccurate information.

THE SOLUTION: Streamline risk assessment processes using common frameworks like the NIST Cybersecurity Framework or ISO 27001. Consider implementing automated risk assessment tools to reduce redundant information requests and alleviate vendor fatigue.

11 Risk of Use of AI

THE CHALLENGE: Artificial intelligence deployed by third-party vendors can carry unforeseen risks stemming from the intricate nature of AI algorithms and associated concerns with data privacy and security. AI models can be difficult to interpret, making it challenging for risk assessors to understand how decisions are made and assess the reliability of results.

THE SOLUTION: Educate risk assessors on AI technologies and their assessment methods. Use tools and techniques for model explainability to improve the transparency and interpretability of AI models and conduct independent audits and reviews of AI-based risk assessment systems to validate the accuracy, fairness, and reliability of results.

12 Prioritizing Remediation Efforts

THE CHALLENGE: Evaluating risks is only the first step. Prioritizing and coordinating remediation efforts across a vast third-party ecosystem can be overwhelming.

THE SOLUTION: Leveraging scoring methodologies and a project management framework in conjunction with vendor collaboration is the best path forward. Collaborate closely with vendors to establish clear timelines and track progress on remediations.

TPRM demands a strategic approach and specialized tools. Let DLA's cybersecurity experts shoulder the burden, allowing you to focus on your core business. Our services provide the resources and expertise to effectively manage your third-party risks, giving you peace of mind in an ever-evolving threat landscape.

For more information about how we can help you navigate TPRM challenges, contact us here.