SPOTLIGHT
Sponsored by: AuditBoard

**With the increased prevalence of third party–related cybersecurity breaches and subsequent legislative action, third-party risk management platforms provide organizations with a tool to manage these emerging risks more efficiently.**

# Beyond the Organization: Managing Risk and Compliance in Third-Party Relationships

*December 2022*

**Written by:** Amy Cravens, Research Manager, GRC and ESG Management and Reporting Technologies

## AT A GLANCE

### KEY STATS

- 90% of organizations were impacted by a supply chain cybersecurity breach in 2022.
- From a trust initiative perspective, third-party risk is a top-ranking risk initiative for over one-third of organizations.
- The top third-party risk concerns for organizations are revenue impacts, operational disruption, privacy breaches, and regulatory fines.

## Introduction

SolarWinds, Log4j, Kaseya: All are security incidents that have been in the headlines over the past several years; all are security incidents that resulted from third-party breaches. The frequency and severity of third-party breaches are on the rise. Organizations are constantly challenged to fend against the potential of a security breach tied to one of often hundreds of third parties with which they engage. In the past year alone, organizations have had numerous serious threats to navigate, including:

- **GitHub:** The incident involved a bad actor cloning and adding malicious code to over 35,000 GitHub repositories while keeping the code's original source code. GitHub, as well as other affected companies, were compromised after the attacker stole authentication tokens from two other upstream software firms.
- **Illuminate Education:** In January 2022, various school districts across the United States had sensitive data compromised as a result of a cyberattack launched on the software provider. Potentially up to 5 million student records were affected by the breach.
- **Toyota:** In October 2022, Toyota discovered that a portion of the site source code of its T-Connect connectivity app was mistakenly published on GitHub and contained an access key to the data server that stored customer email addresses and management numbers. The breach affected nearly 300,000 customers.

## Legislative Response

With the frequency and severity of third-party breaches increasing, security frameworks and supply chain legislation are evolving to minimize the impact of these events. The intention of these efforts varies with both carrot (providing guidance in avoiding breaches) and stick (penalties levied if such breaches occur) approaches being pursued. These initiatives are targeting third-party risk at regional, national, and supranational levels. Regulations emerging specific to the United States include:

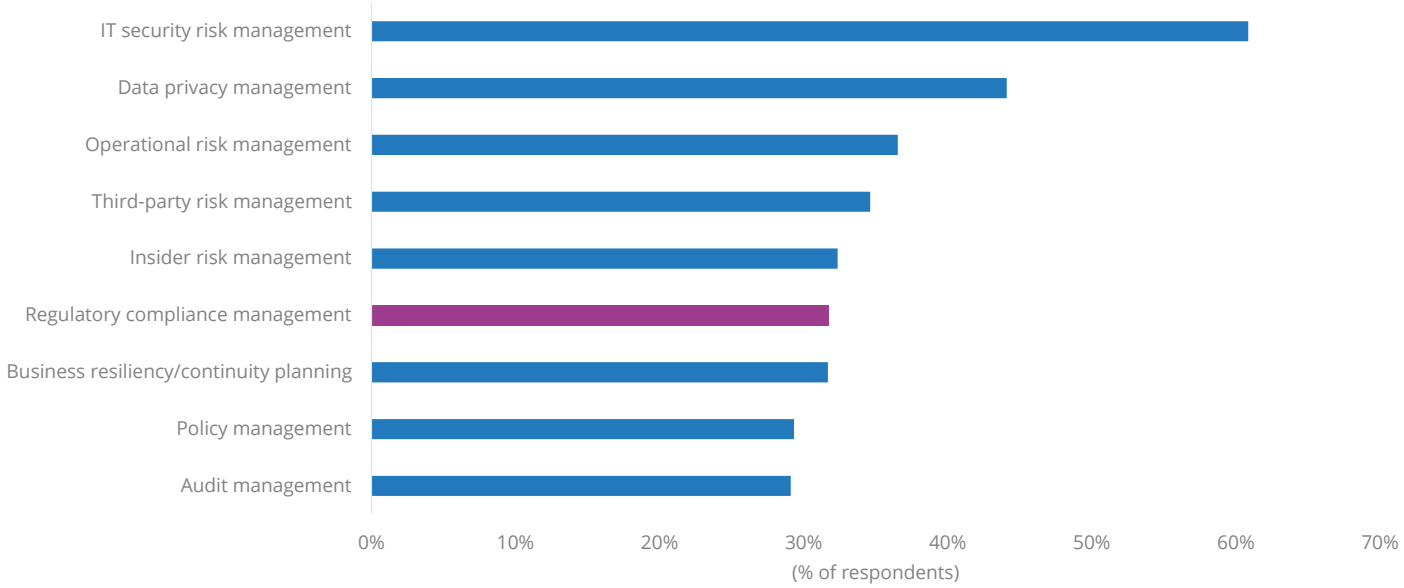
- **Executive Order (EO) 14028 Improving the Nation's Cybersecurity:** The Executive Order on Improving the Nation's Cybersecurity issued in May 2021 mandates that highly regulated industries require software vendors to generate a software bill of materials (SBOM). The intention of EO 14028 is to enhance the software chain integrity of government contractors by establishing baseline security standards for software sold to the government.

- **Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST Special Publication 800-161 Revision 1):** Issued as a response to EO 14028, this update to NIST's cybersecurity supply chain framework guides organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations, specifically highlighting the vulnerabilities not only of a finished product but also of its components.
- **Securing Open Source Software Act of 2022 (Senate Bill S.4913):** Introduced in September 2022, this pending legislation mimics EO 14028 in some aspects while focusing on open source software quality and its supply chain. Unlike EO 14028, however, if passed, S.4913 would remain in force despite administrative changes.
- **Securities and Exchange Commission (SEC) Cybersecurity Proposed Policy:** In March 2022, the SEC proposed amendments to disclosure rules surrounding cybersecurity risk reporting. The proposed amendments would require current reporting about material cybersecurity incidents as well as periodic updates on previously reported incidents. The proposal also highlights the disclosure of cybersecurity governance and risk oversight by the board of directors.

The current environment of heightened third-party software attacks and subsequent legislative response is elevating third-party risk management (TPRM) as an organizational priority. Modern organizations are increasingly focused on managing business risk to foster resiliency and trust; however, much of the risk that an organization contends with is not internal but stems from third-party relationships. Organizations rely on third-party suppliers for products and services necessary to operate; however, these relationships inherently introduce risk to organizations. IDC research has found that third-party risk is among the top considerations for organizational risk management, ranking just below internal IT security, data privacy, and operational risk (see Figure 1).

FIGURE 1: ***Benefits of Automating Third-Party Risk Management***

**Q** ***Which of the following risk management-related areas are most strategic to your organization's trust story?***



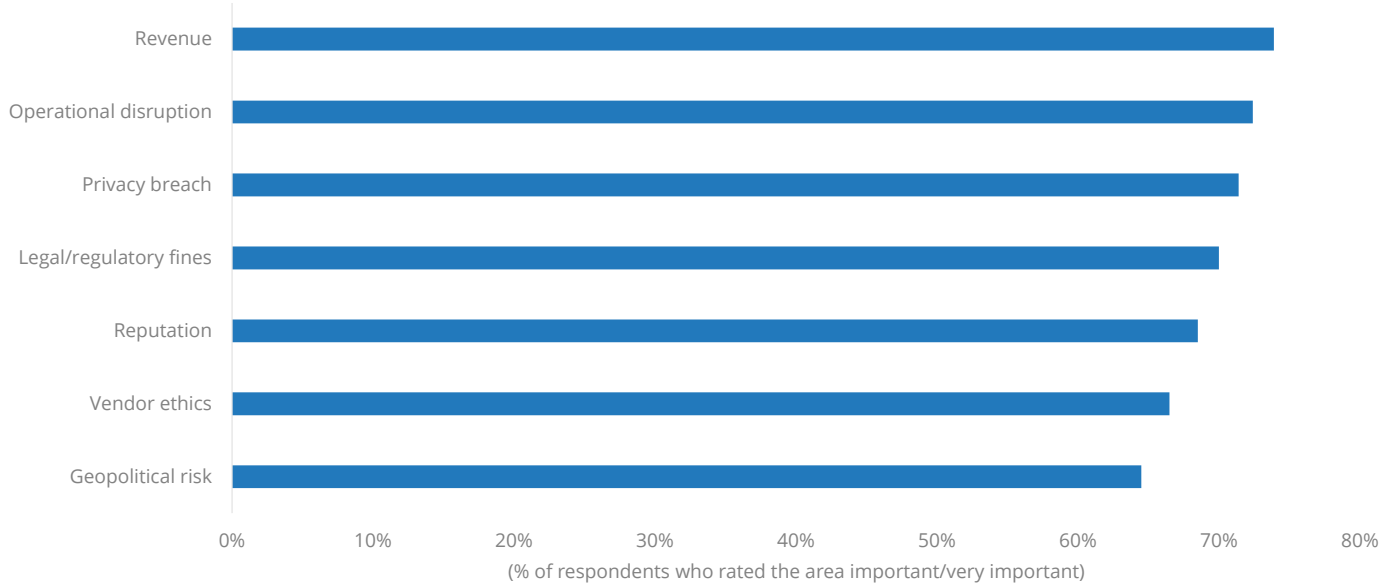

*n = 507*

*Source: IDC's Future of Trust Survey, February 2021*

Third-party risk is particularly important in an organization because failure to secure third-party relationships will directly impact other aspects of organizational risk: A third-party breach can jeopardize internal security and privacy measures as well as disrupt operations and result in regulatory fines. In fact, these are the very concerns that organizations have prioritized regarding third-party risk. According to IDC research, the top third-party concerns among organizations are revenue impacts, operational disruption, privacy breaches, and regulatory fines (see Figure 2). Third-party risks are, in essence, a microcosm of enterprise risk with the same concerns of breaches, compliance, fines, and reputation; the differentiator is that those risks come in through a third-party relationship and thus are more difficult to manage.

FIGURE 2: ***Top Areas Related to Third-Party Risk***

**Q *How important are each of the following areas related to third-party risk?***




*n = 203*

*Source: IDC's GRC Implementation Survey, July 2021*

## *TPRM Response*

TPRM solutions support organizations in managing the myriad of risks across hundreds, or thousands, of third-party suppliers. The information management and automation benefits that TPRM solutions deliver result in increased efficiency and efficacy in vendor risk analysis, which, in turn, reduces the potential for a risk event to occur. Among the key capabilities that TPRM solutions offer in preventing a third-party security breach are:

- **Vendor inventory:** The first step in managing third-party risk is to identify an organization's vendors and chronicle those vendors in a central repository. TPRM solutions can support an organization's efforts to inventory vendors and leverage this inventory with applied intelligence to launch assessments and other monitoring/remediation efforts.
- **Vendor screening/due diligence:** TPRM solutions automate initial vendor assessments, questionnaires/surveys, and risk rating. Automating vendor due diligence typically reduces vendor assessment time by 30–50%, which is a significant savings across a network of hundreds of vendors.

- **Software bill of materials:** Organizations can leverage TPRM software to continuously monitor SBOMs and minimize risk. A secondary application of automated vendor screening is to collect information during onboarding (either via surveys or open source lists) of the "ingredients" in a software solution. By ingesting this detailed information, when security issues arise, organizations can quickly assess which of their software vendors may be impacted by the issue and begin remediation efforts.
- **Third-party risk categorization and assignment of key controls:** TPRM solutions assess and rank vendor risk, basing the level and frequency of review on this risk rating. This automated analysis can also determine which questions should be included in the due diligence process, eliminating unnecessary information collection and thus improving efficiency for both the client and its vendors.
- **Risk/compliance monitoring (continuous monitoring):** While due diligence review and onboarding assessment help organizations select the best partners at the moment, risk is fluid, and a trusted partner can become a risk very quickly. Even when vendors are reassessed at regular intervals, significant risk events require immediate remediation, reducing the efficacy of this type of risk management. For this reason, vendors must be continuously assessed across risk parameters. Integration with news monitoring and risk scorecard services supports this continuous assessment. A risk management platform that automates risk notices based on risk events identified by these services helps organizations better identify and respond to vendor risk.
- **Automated alerts/workflows/risk response:** A key component of TPRM solutions is automation of notifications and remediation of risk using preset parameters linked to various risk controls. When vendors fall out of compliance with a particular control, workflows are commenced that alert the appropriate responders, and the risk is remediated.

## *Considering AuditBoard for Third-Party Risk Management*

AuditBoard provides an integrated audit, risk, and compliance management platform to some of the largest global organizations. With a foundation in SOX compliance, the platform has rapidly transitioned over the past two years, expanding into other risk and compliance modules, including RiskOversight, CrossComply and, most recently, ESG and TPRM. AuditBoard's new TPRM solution draws on developed expertise in managing risk and compliance concerns internal to an organization and projects that learning to external parties, including vendors, partners, or customers. As with other AuditBoard modules, the TPRM solution streamlines, automates, and provides assurance of external parties' IT security posture. Capabilities include:

- **Profiling:** Potential vendors are assessed based on the nature of the relationship and their access to information or customer data.
- **Due diligence:** Questionnaires for due diligence are based on the initial profiling tier, accounting for the vendor's product, the relationship type, and the access to customer data. Vendor assessments can be customized so that an enterprise's risk strategy can be reflected in the TPRM risk assessment. Based on the risk assessment and the vendor's risk tier, the platform will recommend appropriate assessment questionnaires and management controls. Questionnaires can also be automated based on predefined qualifiers or events. Vendor reassessment can also be automated, again linked to tier and profile, which will determine the frequency and detail of reassessment.

- **Workflows:** The platform automates the collection of compliance reports and triggers risk workflows when a vendor issue arises.
- **Reporting:** Dashboards present real-time assessment of vendor population from which reports can be automatically generated. TPRM dashboards and reports are presented as a layer of the total cyber-risk report and will highlight the riskiest vendors (and associated organization departments) and common control failures.

### *Challenges*

Third-party risk is an especially challenging area to holistically capture due to the involvement of multiple organizational departments as well as the broad scope of risk. While IT security risk is an important element of assessing a vendor or a supplier, other factors contribute to the total risk landscape for that vendor or supplier, including procurement risk, non-IT compliance risk, financial risk, geopolitical risk, and ESG risk.

Often, each of these risk types is being assessed by a different department within an organization, but these risk lenses are seldom unified in a consolidated vendor risk analysis. Holistic GRC platforms offer the potential to bridge the gap between isolated vendor risk assessments to migrate toward a broader spectrum of vendor risk analysis.

## *Conclusion*

The breadth of third-party risk is becoming increasingly expansive, and the implications are more impactful than ever before. IT security risks continue to loom large; it is estimated that 90% of organizations were impacted by a supply chain cybersecurity breach in 2022. The consequences of this broadening third-party risk landscape are elevated by the introduction of new legislation mandating better management of third-party vendors. To address these third-party risk and compliance issues in an efficient and effective manner, organizations should look to TPRM platforms that provide detailed scrutiny of vendor partners as well as the ability to quickly respond to developing risks.

# About the Analyst

***Amy Cravens,*** *Research Manager, GRC and ESG Management and Reporting Technologies*

Amy Cravens is Research Manager for IDC's Security and Trust Group responsible for the Governance, Risk, and Compliance (GRC) Technology practice. Ms. Cravens will be responsible for research related to the innovation and transformation of Governance, Risk, and Compliance software including analyzing technologies aimed at solving fraud, third-party risk, and other types of risk across the enterprise.

## MESSAGE FROM THE SPONSOR

### More About AuditBoard

AuditBoard is a leading cloud-based platform transforming audit, risk, ESG, and compliance management. More than 35% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fourth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit: www.AuditBoard.com.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

**IDC Research, Inc.**
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com