Prevalent™

The Path from Reactive to Proactive Third-Party Risk Management

Table of Contents

Reactive Third-Party Risk Planning is a Slippery Slope

An organization's supply chain can change on a daily basis. Business partners need access to sensitive information to help a company achieve its goals, and vendors supplying critical components and services require APIs and network access. Some of these third parties may be long-term and trusted partners, while others may be relatively unknown and based across the world.

While it seems obvious that organizations need to up their games and plan proactively for third-party risk in their security programs, many organizations slip up by taking a reactive or ad hoc approach. In a 2019 study, the Ponemon Institute found that almost 1 in 5 organizations surveyed only review their third-party risk management programs after a third party has a security incident, and 23% had no schedule at all for reviewing their programs and policies. That means over 40% of organizations aren't performing basic due diligence – on what many see as the greatest security vulnerability.

1 in 5 organizations
only review their third-party risk management programs after a third party security incident, and 23% had no schedule for reviewing their programs and policies.

-Ponemon Institute study

The lack of proactive planning can have costs. Irrespective of the attack vector, the responsibility for protecting sensitive information – and the consequences of a breach – remain with the owners of the information. Regulatory standards like HIPAA, GDPR, the California Consumer Privacy Act, and Section 5 of the FTC Act require the protection of sensitive information. This responsibility cannot be "outsourced" to a vendor – you can outsource the operation, but you can't outsource the risk.

Many companies have learned this the hard way:

- California-based Cottage Health had a **$4 million cyber insurance claim denied** and later paid a $3 million **HIPAA settlement** when their IT vendor **exposed information on over 32,000 patients.**
- Mobile phone manufacturer **BLU Products** as a company and its CEO as an individual settled a "false and misleading" claim with the FTC under section 5 after it was discovered that the China-based company providing over-the-air update software to BLU could also capture personal information from the phones. As part of the settlement, BLU must submit to third-party assessments of its security program **every two years for 20 years.**
- The 2017 Equifax breach also shows that security has become a board-level issue; it reduced the company's market capitalization by over 30% and resulted in the **forced retirement of the CEO, CIO, and CSO.** The company's reputational damage continues today.
- Quest Diagnostics faces a **class-action lawsuit** seeking over $5 million for the breach caused by their third-party billing company, American Medical Collection Agency.
- Wendy's agreed to pay a **$50 million settlement** after a breach of their third-party point-of-sale equipment vendor.

Why Third-Party Risk Management is a Problem for Most Organizations

Risk assessments are a part of any security professional's process. A risk assessment requires understanding an organization's business goals, the application or system being assessed, and any internal policies or external regulatory requirements covering the system. Security teams, software architects, business owners, and developers can then identify risks to those systems and assign controls to mitigate those risks. When a risk assessment involves a third party like a partner or vendor, there are several factors that can complicate the accuracy of the assessment.

1

Lack of Consistency

In most organizations a risk assessment is a manual process. The typical approach involves lengthy, spreadsheet-based questionnaires for internal and external teams. Once completed, security and compliance teams aggregate the responses, identify gaps, and provide all parties with controls to implement. Without strict program controls, different individuals or teams may identify different risks for the same project and controls will lack consistency.

2

Lack of Resources and Limited Scale

Assessments are time-consuming exercises requiring participation from scarce security resources and expensive engineering and compliance experts. Completing thorough assessments, even for projects that are entirely in-house is expensive and represent snapshots of a vendor's security profile at the time of the assessment – one that can change overnight with changing personnel and policies or the disclosure of a new vulnerability. Even when teams need to assess just their top-tier vendors, the task can quickly become impossible to manage at scale.

3

Limited Available Intelligence

Conducting an assessment without considering threat intelligence provides only partial risk information. Most spreadsheet-based assessments use numeric or contextual (e.g., high, medium, low) "scores" that are rarely based on granular criteria that weigh controls or intelligence on the changing threat environment. Continuous monitoring can address this, but it seldom occurs because of the complexity of the third-party ecosystem.

9 Reasons Organizations Struggle to Achieve Their Third-Party Risk Management Objectives

Prevalent surveyed dozens of organizations in-depth to understand specific challenges in scaling and managing third-party risk management. The study found critical risks around each five pillars of third-party risk management: Content, Roles and Responsibilities, Coverage, Remediation and Governance.

Content Risks

Not Creating a Centralized Risk Register – The key to any risk assessment initiative is to measure all critical factors as accurately as possible and creating a centralized tool for reporting. In a third-party risk assessment, this means ensuring that questions are answered consistently between vendors and partners. Managing risk through individual spreadsheets can be inconsistent and unreliable and creates extra work during audits. It also makes it difficult to identify risk trends across multiple third parties.

52%
didn't have a standard way to present risk data

Roles and Responsibilities Risks

Lacking a Standardized Process – 62% of the survey respondents identified the absence of program operational manuals and standard scoring mechanisms in their third-party questionnaires. Without a guide for assessment workflow, key risk factors could be missed, particularly as new personnel join a team.

62%
lacked a standardization process

Failing to Examine Resource Requirements – Insufficient resource planning was cited as a risk by over half of the respondents.
An effective third-party risk management program requires time from security, partner management, and business owners. Teams that do not accurately evaluate a) the number of third parties requiring assessment and b) the effort required in people and time for each assessment will struggle to meet their objectives.

52%
had resource planning shortfalls

Using Expensive Resources for Simple Tasks – Managing an assessment requires personnel to issue questionnaires and confirm that the third parties have responded to all queries completely. When these tasks fall to scarce and expensive security personnel, the cost of an assessment rises and other, higher-order security tasks suffer.
59% of the respondents believed their organizations did not minimize costs of assessments by assigning oversight responsibility to an "operational" resource.

59%
overspent on TPRM resources

Coverage Risks

Stopping at Third Parties – Risk is not limited to an organization's immediate (third-party) partners and vendors. Their partners and vendors, so-called "fourth parties," can also introduce risk, as can others further up the supply chain. 79% of survey respondents ranked high the difficulty of identifying those organizations, the corresponding risks introduced by fourth parties, and their ability to prescribe and enforce controls against those risks.

79%
didn't consider fourth-party risk

Remediation Risks

Not Standardizing Remediation Guidelines – 86% of the survey respondents' top challenge was that their organizations lacked a consistent and enforceable set of standards for risk remediation. This can result in each third-party applying unique controls or individual controls that are not in line with organizational or regulatory requirements. Without consistent guidelines, managing dozens or hundreds of vendors is unsustainable.

86%
had inconsistent remediation guidelines

Not Scoring Risk Likelihood and Impact – Risk is a function of the potential impact of a threat and the likelihood of an attack. Without understanding the likelihood of a successful attack and impact on an organization's goals, teams cannot respond consistently and efficiently. In the study, 59% of organizations cited this challenge. Monitoring threat intelligence will help rank risks appropriately and reassess risks over time.

59%
had incomplete risk scoring mechanisms

Governance Risks

Limiting Risk Reporting to Tactical Uses – The goal of performing third-party risk assessments is to identify and mitigate issues that could result in a breach or accidental loss of sensitive data. While reports on individual third parties are obviously useful, 69% of survey respondents stated that key risks, observations and commonalities of risks across the program were not used to drive strategic conversations about new and emerging threats or to inform changes to their internal assessment and risk remediation approaches.

69%
were missing strategic reporting opportunities

Lacking a High-Level Understanding of Third-Party Risk – 59% of respondents struggled to gain an overall view of third-party risk. If an organization views each third-party in isolation and "siloes" reports, then it is not possible to provide a full and accurate picture of program findings, observations and key areas of risk back to an organization. It is better to aggregate information to identify common risks, then plan to defend against those risks in an efficient manner.

59%
struggled to gain an overall view of third-party risk

How to Start

Traditional, manual third-party risk assessment programs are slow, inconsistent, and cannot scale to keep pace with increasing regulatory demands.

> **Taking the right approach can lower overhead and reduce demands on security and compliance personnel.**

Standardize Risk Assessments and Scoring

The first step in a risk assessment is to first understand applicable regulatory standards and then translate those requirements into clear, consistent questions for vendor surveys. Additionally, organizations must define scoring criteria to identify acceptable controls and evidence from third parties. Industry-standard risk assessment surveys such as Shared Assessments' Standard Information Gathering (SIG) and NIST can be used as is or modified to meet an organization's needs.

A defined set of requirements, controls, and scoring addresses the top concern of survey respondents and brings consistency to reporting. In addition, it better satisfies auditors' needs for validation. Defining criteria for each third-party 'tier' or service type featured within scope of the program ensures that security measures are appropriate for the risk posed by each service type.

Standardization can also address roles and responsibilities for surveys, assessments, and overall program management. This optimizes the organization's return on investment from security and compliance personnel and increases the ability to predictably reproduce the program with new people and projects.

Account for Fourth Parties

As noted earlier, risk does not end with third parties, and attackers are adept at finding soft targets. A mechanism for identifying and mapping fourth parties can be incorporated into the assessment process by understanding which entities could have an effect on key organizational risk impact areas, such as continuation of services, finance, reputation, and quality of services.

Leverage Reporting to Mature Programs

Standardizing scoring helps prioritize risks and mitigation efforts by and between suppliers and partners. Aggregating that data across all third parties can help identify key events for consideration within program strategy sessions and across broader cybersecurity initiatives.

Moving From Reactive to Proactive Third-Party Risk Management

Get Started Quickly with Access to a Library of Comprehensive and Standardized Vendor Intelligence Profiles

Improving and maturing a risk assessment program from reactive to proactive need not be slow or expensive. Organizations can quickly improve their security profile by focusing on their most critical partners. A simple, low-cost entry method is to leverage the existing networks of vendor surveys. These include thousands of completed standardized vendor questionnaires backed by continuous monitoring to ensure the survey responses remain valid. Vendor libraries enable companies of all sizes to reduce time spent on developing surveys and gathering vendor risk data, and instead focus on risk analysis and remediation and scaling a third-party risk management program.

Scale Your Program with Vendor Risk Assessment Services

Building internal third-party risk management requires time and expertise. For organizations requiring more structure and assistance, vendor risk assessment services provide third-party risk management as a service. Organizations benefit from experienced risk management experts who design surveys, collect vendor evidence, review assessments for completeness, identify risks, and provide remediation guidance on your behalf. Third-party risk assessment experts can guide the program, customize surveys, monitor compliance, produce reports, and help mature the program over time.

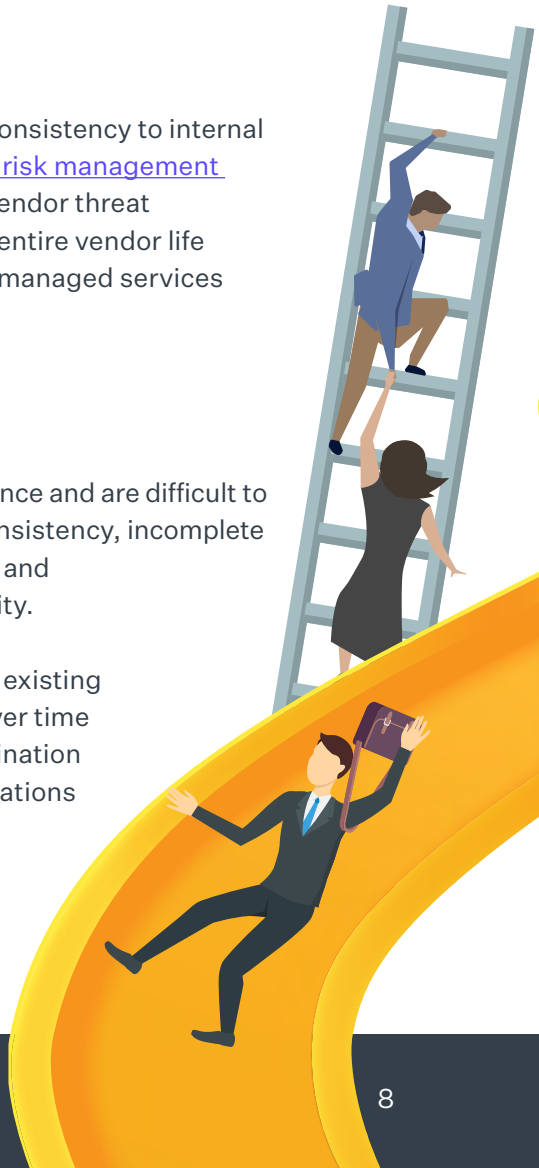
Improve Consistency with an Agile, Repeatable Model

Automated software solutions can bring all the benefits of speed, scale and consistency to internal teams, replacing reactive and manual processes. A cloud-based, third-party risk management platform combines automated, standardized vendor risk assessments with vendor threat monitoring, assessment workflow, and remediation management across the entire vendor life cycle. If external assistance or expertise is helpful, professional services and managed services can optimize and mature a vendor risk management program.

Improve Your Program Maturity

Manual third-party risk management programs lack speed, scale, and intelligence and are difficult to manage, monitor and improve. As shown by the survey, they suffer from inconsistency, incomplete assessments, and sub-optimal results. Lacking intelligence on current threats and a changing environment, manual processes provide only the illusion of security.

Reaching third-party risk assessment maturity can start easily by leveraging existing networks of assessments with continuous monitoring. Increasing maturity over time can be accomplished through managed services, in-house teams, or a combination of the two. Moving to an automated and cloud-based approach takes organizations from being reactive to proactive, and from ad-hoc processes to intelligence-driven risk assessments and continuous improvements.



Take the Next Step

If you're unsure where your organization is on the TPRM maturity scale, sign up for a **free Maturity Assessment consulting session**. You'll walk away with an in-depth report on the state of your current program, plus practical recommendations for how to bring it to the next level.

Pressed for time?
Answer 10 multiple-choice questions to get an instant "gut check" of your your organization's third-party risk readiness.

About Prevalent

Prevalent takes the pain out of third-party risk management. Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors, suppliers and other third parties. Our customers benefit from a flexible, hybrid approach to TPRM that's powered by three core solutions:

- The Prevalent Vendor Intelligence Network is a library of on-demand risk reports for over 10,000 vendors, based on completed assessments and continuous threat monitoring across 200+ sources.
- Prevalent Vendor Risk Assessment Services provide white-glove outsourced TPRM, handling everything from onboarding and assessments, to risk analysis and remediation management.
- The Prevalent Third-Party Risk Management Platform is a cloud-based solution that unifies and automates vendor management, assessment and monitoring for a 360-degree view of risk.

Our team works closely with each customer to tailor a solution that not only fits their unique needs, but delivers a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.

To learn more, please visit www.prevalent.net.