What’s the Purpose of Third Party Risk Management?

Your company deploys advanced IT security controls and follows best practices to prevent unauthorized access to your systems and protect sensitive company and customer data. Unfortunately, it’s not enough. It’s not enough because there is an entire spectrum of risks you don’t directly control — access to your systems and sensitive data by your vendors. Simply stated: the overall security of your data and systems is dependent on the risk controls provided by your vendors.

A recent Vendor Vulnerability Index research report released by Privileged Identity Management company Bomgar, showed that breaches occurring from third parties account for two-thirds of the total number of reported breaches.\(^1\)

In addition, the study found that:

- **89 vendors** on average, are accessing a company’s network every week
- **Only 46%** of US companies said they know the number of log-ins that could be attributed to vendors
- **Less than 51%** enforce policies around third party access
- **69%** said they definitely or possibly suffered a security breach resulting from vendor access in the past year

Studies like this and many others over the past few years have driven the consensus among security professionals that the risk posed by third parties is not only substantial, but it is increasing, and there is no “one size fits all” solution to the problem.

This is why you need a comprehensive approach to your Third Party Risk Management (TPRM) program that allows you to:

- **Identify** the security controls a vendor must have based on the services they provide
- **Determine** if they are maintaining those controls
- **Develop** plans for corrective action to be taken by the vendor
- **Monitor** the vendor’s threat environment for additional external risks and operational issues
- **Reduce** collection time by leveraging shared, standardized risk information collected for other companies who utilize the same vendor

\(^1\) Bomgar. Vendor Vulnerability Index brings security risk of third-parties to light, April 2016
Why is Third Party Risk Management So Complicated?

TPRM is a growing concern for the CISO, CIO, CEO, and even Board-level stakeholders. In fact, Gartner recently stated in their June 2017 Magic Quadrant for IT Vendor Risk Management that by 2020, 75% of Fortune Global 500 companies will treat vendor risk management as a board-level initiative to mitigate brand and reputation risk.

In addition, with the introduction of the Internet of Things (IoT), organizations are quickly realizing that they are not prepared, and according to a recent Poneman and Shared Assessments study, are still “relying on technologies and governance practices that have not evolved to address emergent IoT threat vectors.” Even though 25 percent of respondents in this study stated that their board of directors require assurances that IoT risk among third parties is being assessed, managed, and monitored appropriately, only 27 percent said they have the resources to support it.

The reality is that once your data is under the control of your vendors, it’s still YOUR data. It is up to you to ensure your vendors have adequate security controls in place and that they keep those controls current based on the ongoing changes to the threat environment. Further complicating this, are many vendor variables that you need to consider, such as:

- Whether the vendor has custody of, or access to, your sensitive information
- Whether the vendor has access to your company’s network
- Size of the vendor
- Location of the vendor
- Sophistication of the vendor’s IT and security teams
- Whether the vendor itself outsources services
- The vendor’s product or service
- Regulations

Other factors to consider include geography, recent events relating to the vendor (e.g. a data breach, bankruptcy filing, lawsuit, leadership change), and any number of other variables unique to the millions of vendors in business globally.

What does this vendor relationship complexity mean for security professionals responsible for third party risk management? In short, they need several tools to efficiently gain visibility into and manage the risk of their vendor ecosystem.

---

2 Gartner. Magic Quadrant for IT Vendor Risk Management, June 2017
3 Poneman Institute. The Internet of Things (IoT): A New Era of Third-Party Risk, May 2017
One Size Doesn’t Fit All

Vendor assessment must be ‘fine-tuned’ to the type of data involved, the systems being accessed, and the nature of the services provided by the vendor. For example, would you ask a 15-person law firm that handles your patent filings and litigation to complete the same comprehensive questionnaire they send to a cloud-based application provider? Would a healthcare company ask their laboratory analysis vendors the same set of risk questions they would their payroll company? How much do you really care about the security controls of the vendor that landscapes your company grounds? Software Development Life Cycle (SDLC) processes are obviously important for vendors delivering applications embedded in your organization’s operations, but they’re irrelevant to a claims processing vendor of a car insurance company.

Once the proper scope is established, assessment due diligence must be requested from the vendor, validated, and then analyzed. Upon completion, decisions are then made about risk acceptance and/or mitigation. Results must be consolidated and reports generated to senior management that define outsourcing risk and the operational efficiency of the TPRM process. This effort - extended over dozens, hundreds, or even thousands of vendors - is essentially impossible to conduct without software automation.

Vendor Assessment Software

Assessment (upper case “A”) has become the go-to word in the third party risk world, but whether a formal Assessment is appropriate for a vendor or not, the requirement to assess (evaluate, appraise, gauge, estimate, determine, etc.) the risk of the vendor doesn’t go away. Multiple options are needed to have a successful TPRM program.

Fortunately, technology is evolving to provide exactly such options for the growing third party risk community. First, automated Assessment tools are significantly more sophisticated than their predecessor generations. Today’s vendor risk management software offers the kinds of features that enable vendor content tuning, including:

- Ability to “tier” vendors, or determine which surveys and other requests to make of vendors based on their relationship to the organization
- Ability to pull completed and reviewed standard content from vendor evidence networks, saving both the vendors and your organization countless hours of time
- Ability to build custom, supplemental surveys that address the gaps in standard content
- Risk score flexibility to enable users to customize to their risk needs within the tools
- Shipping with off-the-shelf, industry-accepted standard content
- Built-in workflows that provide automated and auditable interaction with vendors to facilitate remediation and/or provide greater risk visibility into your vendor ecosystem
Continuous Threat Monitoring

Unlike first generation TPRM continuous monitoring offerings, contemporary offerings provide a holistic view of vendor risk as determined by external events and internal security posture. Rather than focusing exclusively on outdated measures of security provided by external network scans, today’s monitoring products gather risk event data from several sources on an on-going basis to form a risk picture across the vendor’s entire spectrum of potential threats to your organization.

Data breaches are just one way in which your relationship with a vendor can negatively impact your operations and external network scans provide little insight into a vendor’s vulnerability in today’s sophisticated threat environment. Financial risk events, operational challenges (such as natural disasters or leadership shake-ups), regulatory citations, fraudulent practice claims, and lawsuits are just a few examples of the kinds of events that can greatly impact the risk of a vendor to your organization. Fortunately, options exist in advanced TPRM solutions for third party risk professionals to keep track of their vendors on a daily basis, beyond the narrow focus of first-generation monitoring tools with a narrow-minded view of risk.
Evidence Sharing Networks

A relatively new innovation in third party risk is providing third party risk managers with all of the benefits of the traditional Assessment process, but with much less aggravation. The advent of Vendor Evidence Sharing Networks is making completed, verified, standard surveys available to organizations while eliminating the tedious time-and-resource consuming process of collecting accurate data from vendors.

The “Complete-Once, Share-Many” model of vendor sharing networks means the burden on vendors is similarly alleviated. By greatly reducing the effort required to collect or complete surveys, it means that both first and third parties can spend much less time gathering controls data and much more time on what’s important: working together to decrease control gaps and reduce overall risk.

Evidence network sharing is a feature built into advanced vendor risk management software, so that users can not only leverage advanced workflows, reporting, scoring, and other features of these enterprise software solutions, but can also augment that rich functionality with “off-the-shelf” vendor evidence that can instantly form the foundation of a comprehensive and effective third party risk management program.
Mixing and Matching Capabilities to Meet Your Program Needs Today and Tomorrow

Very rarely will only one of the three solutions discussed in this whitepaper satisfy the TPRM needs of an organization with such diverse vendors — and that’s exactly the point. Having the access to all three components is necessary to build a highly-functioning, efficient third party risk program — and Prevalent is the only vendor in the market today that can provide all three advanced solutions. Prevalent developed the first purpose-built Third Party Risk Management cloud-based platform in 2012 and is the only company that offers a complete, integrated suite of solutions that includes automated assessment software, continuous threat monitoring, and innovative vendor evidence sharing networks.
Recently named a Leader in the Gartner Magic Quadrant for IT Vendor Risk Management, Prevalent helps global organizations manage and monitor the security threats and risks associated with third- and fourth-party vendors.

Prevalent introduced the only unified platform for Third-Party Risk Management and the first vendor evidence sharing portal that enables collaboration between both enterprises and vendors. Prevalent is the chosen platform powering the NH-ISAC CYBERFIT® Shared Risk Assessments program and was named the Fastest Growing Cybersecurity Company by the 2017 Cybersecurity Excellence Awards.

For more information, please visit www.prevalent.net, email info@prevalent.net or call 877-PREVALENT.