

# Best Practices for Reducing Third Party Risk

By Brad Keller, Senior Director of 3<sup>rd</sup> Party Strategy

The simple truth is that the security measures organizations put in place are not enough to protect them from threats. Third parties can present the greatest area of risk exposure — both for data security and for regulatory compliance. It is much easier for hackers to penetrate smaller third party vendors to get to larger business partners with more robust controls.

## Knowing the Risks

As organizations increasingly outsource non-core business processes, customer and proprietary data move beyond their direct control, along with access to critical systems. Once you are no longer directly responsible for controlling access to systems and those who touch your data, you lose visibility into all the places it can go. This has a spider web effect; companies who outsource often discover that the vendor they're outsourcing to plans to outsource as well.

Not knowing where your data is doesn't just pose security problems, it has potential regulatory impact. Regulatory pressure around data protection and data privacy is increasing, and the ramifications of non-compliance broaden significantly when you think about all the third parties that are essential to your daily operations. The advantages of the cloud — having data go wherever it can effectively be managed and used at the time — also creates problems. There may be substantive regulatory impacts when data moves cross-border. Many organizations must know if their data leaves the U.S., and if their European Union (EU) data leaves the EU. You can't always assure that with a cloud provider. Vendor termination also poses a problem. When you sever a vendor relationship, it is important to ensure that your data is either returned to you or destroyed. Because of how cloud data is stored, that's not always possible.

An effective third party risk management program is essential not only to compliance efforts, but to your overall security posture.



### A Growing Problem

An average of **181 vendors** access a company's network every week, according to a recent report by Bomgar. This is more than double the number from 2016.

### Do You Know Your Vendors' Security Posture?

A Ponemon Institute survey of nearly 600 professionals at organizations with a vendor data risk management program revealed that **only 38 percent** evaluate the security and privacy practices of all vendors before starting a business relationship that requires the sharing of sensitive or confidential information.

## 10 Best Practices for Success

1

### **Invest Time in Foundational Elements**

Too often, when companies set out to assess vendors, they rush into developing a questionnaire and initiate assessments without having created the framework for doing so. It is important that the foundational elements of a successful program — policies, procedures, a comprehensive vendor inventory, and the appropriate way of contracting — are well-established. To do this, the right stakeholders need to be involved. Vendors are the partners of the business unit and need to be treated accordingly by the group that conducts risk assessments. Vendors must be comfortable with the process, understand what has to be done, and help to determine what happens when controls aren't found to be in place.

2

### **Look at it as a Lifecycle**

Organizations sometimes develop inaccurate expectations about the scope of third party risk initiatives. Develop your program to make sure that you address the entire lifecycle of your vendor relationships — from selection, to onboarding, to management to termination — and carefully evaluate the cost and effort involved in each step.

3

### **Engage in Vendor Prioritization**

It is critical to have a current vendor list that includes the services they provide, the data they access, and the criticality of their services (from an availability standpoint). Which vendors you need to assess, and what you need to ask them depends on who they are, and what they do for you. Vendor risk framing starts by assigning a risk rating to the type of service being provided. Start with the risk that is inherent with outsourcing that function. Consider that risk and the security and data protection requirements that need to be placed on any company that's going to provide that service. That is the inherent risk calculation that will help to place them in the right risk categories.

4

### **Get the Contracting Right**

A vendor contract is the playbook that details what you can do throughout the relationship. Alignment and synergy need to exist between the contracting process and the people who understand and can define what the risk requirements need to be for that type of service. Whomever is responsible for the contract (Legal, Procurement etc.) should be aware of the provisions required to address the risks associated with the services provided by that vendor. All contracts are not equal; vendors need to be held to different accountability standards based on what they are providing.

5

### Assess Your Maturity

Evaluating the maturity of your program is essential. One area may be more evolved than another. For example, if you're in a regulated industry such as financial services, the part of your program that is subject to regulatory requirements needs to be more mature than it would be if you were in an unregulated industry. Assess the maturity of the different pieces of your program and decide which of them need attention.

6

### Look at Reporting from the Top Down

Don't start the reporting process by trying to figure out what data you need to gather. Start by considering all of the reports you have to deliver and who you need to deliver them to. Then you can easily work backward to determine what data you need. There are two central areas to report on — risk and operational effectiveness.

- What risk is the company subjected to by outsourcing based on type of service, vendor, or line of business?
- How effective is the program? Operational assumptions and program performance metrics can help demonstrate the effectiveness of your program and why you may need more resources to accomplish your goals.

7

### Leverage Automation

Assessing your third parties can be a time-consuming, manual effort. In fact, 40 to 50 percent of the time spent involves the process of sending out questionnaires, getting answers back, and validating vendor responses and documentation. Automation can free risk assessors from tasks that don't require their skill sets and speed the process up. With an automated solution, an individual assessor can easily conduct three to six times as many assessments in a year as they can manually.

8

### Treat Them Like a Partner

Many vendors get assessed often, have good security in place, and don't want to go through the process hundreds of times a year. When the vendor you need to assess is providing something that is critical to delivering your own products and services, be sure to treat them like a partner, rather than simply dictating what they're going to need to do for you. Make sure they understand from the beginning what you're doing, why you need to do it, and what information you need. And when it comes to post-assessment remediation, try to put yourself in the place of the vendor. If they don't have the necessary controls in place, work with your stakeholder business unit to get them implemented but be fair and reasonable in the expectations you place on the vendor.

9

### Assess Consistently

Sometimes the desire to move quickly — so that a vendor's product or service can be delivered and start generating revenue — leads companies to initially conduct one level of assessment and then shift to a more extensive version afterward. The problem with this is that may lead you to take on levels of risk you're not aware of. Without a comprehensive assessment, you may later discover that they don't have certain controls in place and cannot meet your requirements.

10

### Monitor External Factors

Vendor assessments provide static, point-in-time perspectives; it is important to also monitor outside the scope of the contract for additional factors that are not part of a normal assessment. Consider the following questions:

- Does the vendor face legal action that could impair their ability to deliver services?
- What is their financial condition?
- Are they involved in breach incidents at locations other than the locations where my work is performed?
- Are they subject to regulatory action (OFAC, FTC, or others)?
- Are their executives subject to SEC investigation?

## Don't Leave Your Company's Reputation in Someone Else's Hands

Outsourcing has clear benefits — from lower costs to increased efficiency and productivity in non-core business processes. But the value third parties bring can be eroded by associated risks. Third party weaknesses are your weaknesses. By developing and maintaining an effective third party risk management program, you can help ensure that your vendors have strong controls in place and protect your organization from fiscal, operational, regulatory and reputational risk.

## The Prevalent Solution

Prevalent helps enterprises manage risk in third party business relationships. It is the industry's only purpose-built, unified platform that integrates a powerful combination of automated assessments, continuous monitoring, and evidence sharing for collaboration between enterprises and vendors. No other product on the market combines all three components, providing the best solution for a highly-functioning, effective third party risk program. As the leader in Third Party Risk Management, Prevalent's actionable intelligence accelerates time to value, improves scale, and increases efficiency across any organization.

For more information regarding Prevalent, visit [www.prevalent.net](http://www.prevalent.net)