White Paper

Third-Party Cyber Risk:
8 Key Considerations

riskrecon™

Contents

 © RiskRecon, Inc., 2018. All rights reserved.

Introduction

Thank you for downloading “Third-Party Cyber Risk: 8 Key Considerations.” In this white paper, we’ll look at why third-party security risk matters, some of the forces transforming this space, and how to prioritize risk. During the way, we’ll dive into principles for fair and accurate ratings and why the security of your vendor’s entire enterprise matters. You’ll also learn the true cost of administering your vendor security questionnaire and how to incorporate continuous monitoring into your third-party risk program. Read on!

Chapter 1: Why Third-Party Security Risk Matters

There are at least three main reasons why third-party security risk matters:

1) Big Impact

Enterprises entrust the protection of their crown jewels—their customer data, their reputation, their finances, and their business availability—with third parties. Are they trustworthy? Why? Why not? What should be done about it? These questions are yours to answer and execute on, because a breach of your third party is a breach of your enterprise.

2) Big Challenges

Third-party risk management is hard. It requires deep transparency, strong accountability, and effective collaboration. Third-party risk has to achieve this position with hundreds and even thousands of organizations while being an outsider to every organization. Additionally, third-party risk has to solve this with limited personnel and resources. This need—to achieve really good risk outcomes from the outside with limited resources—will result in dramatic risk management innovation, key to which will be development of machine learning and artificial intelligence-based risk assessment capabilities. These inventions will occur within the context of third-party risk management and be adopted by enterprises for internal risk management. Necessity is the mother of invention, and the necessity is pressing in a big way.

3) The Greater Good

Third-party risk management is a process of holding enterprises accountable to good security practices. As you improve the security of your third parties you improve the security of the Internet. It decreases the likelihood of data being breached. It decreases the likelihood of systems being turned into DDOS drones or malware servers. It increases the likelihood that systems are going to be consistently available to fulfill their intended purposes. The work of third-party risk management is work for the greater good.

Let's look at the evolving landscape in which third-party cyber risk resides.

 © RiskRecon, Inc., 2018. All rights reserved.

Chapter 2: The Forces Transforming Third-Party Cyber Risk

In the past decade or so, the entire IT application and outsourcing landscape has changed. Back then, most companies relied on relatively small number of IT providers and resellers. Most software and data ran in the company's own data center.

But then, as the delivery of software and services over the public internet (SaaS) became far more efficient and innovative, many companies began shifting from an on-premise software model to the cloud. The initial drivers for adopting SaaS were line of business executives, who could now convert larger capital expenses in smaller, operating expenses. And they could far more quickly implement and achieve desired business results with SaaS than with the traditional approach of installing and configuring software on premise. Over time, many IT departments have also come to prefer SaaS, as they do not have the expertise or resources themselves to maintain the growing number of applications required by business.

Meanwhile, the third-party risk management process has not kept up. Fifteen years ago, companies relied primarily on vendor questionnaires and documentation to determine third-party security risks. And in some cases, the companies would visit the third-party vendor's data center. This worked okay when there were a relatively small number of vendors to be assessed, the company data was still resided on-site, and the vendors themselves had large, sophisticated security teams (e.g., Microsoft, Oracle, EMC, etc.).

Of course, this world no longer exists—but the third-party risk management process has not changed. Now, far more data and systems are no longer on site but at a third-party data center. And in many cases, not at the third-party's data center but at a fourth-party data center. Specifically, a company may contract with a SaaS provider who manages its data, but that third-party SaaS provider often relies on a fourth party such as Amazon or Rackspace to host its systems.

In addition, as line of business now has much easier access to new SaaS technologies, they tend to add more and more of these vendors. Thus, the number of vendors used at a particular company is growing significantly. Unfortunately, many of these SaaS vendors do not maintain big, sophisticated security teams, so their ability to consistently design and maintain good security and data protection practices is more limited.

 © RiskRecon, Inc., 2018. All rights reserved.

Lastly, because it is so simple to sign up SaaS vendors now—often nothing more than a click-through agreement or credit card—many new ones are signed up without even going through the company's formal governance and review process. Therefore, companies work with many vendors with security programs that were not reviewed at all before going live.

Yet with all the growing risk and complexity described above, most vendors return their security questionnaires looking very good. Too good, actually, for an experienced risk or security person to believe, because they are often describing their documented procedures, which can vary considerable from the reality of what they are doing in practice. And both they and the line of business buyer are eager to get through process as quickly as possible so they can go live.

And, even if the process were working, the number of vendors and risk has grown too large to be managed with a manual process of people and spreadsheets. There is no good way to scale the existing process to meet the demands.

Where Does That Leave Us?

Risk professionals are now dealing with three "risk realities:"

1) Their current methods for measuring third-party risk are lacking, at best, and able to capture only a small piece of the actual risk
2) Their current process for gathering and measuring risk is manual, resource-intensive and not capable of scaling to meet the risk reality of their supply chain
3) Most tools—old style questionnaires, newer security rating services—produce laundry lists of issues but no context or prioritization based on actual risk.

No other area of security relies almost entirely on the "honor system" to manage risk. It would be like sending email to all employees, asking them a long list of security questions about their computer. And then entirely relying on their answers without any testing, monitoring, or verification.

Chapter 3: Principles for Fair and Accurate Security Ratings

Companies are increasingly relying on objective risk data and security ratings to better understand and control their third-party risk. Key to those ratings are standards and principles that enable fair and accurate assessments. In recognition of this, in 2017, The U.S. Chamber of Commerce issued "Principles for Fair and Accurate Security Ratings." These ratings are the first-of-its-kind guidelines for an emerging class of solutions that provide objective assessments of third-party security practices. These solutions complement traditional third-party risk management data gathering processes of vendor security questionnaires, attestation document reviews, and on-site assessments.

The principles are the result of a collaborative effort between large American companies (both financial and non-financial) and leading vendor security assessment companies, including RiskRecon.

What Is the Purpose?
The Chamber document itself states: "As security ratings continue to mature, more organizations in the public and private sectors leverage them in making business and risk decisions. As a key piece of a robust security evaluation program, security ratings based on accurate and relevant information are useful tools in evaluating cyber risk and facilitating collaborative, risk-based conversations between organizations."

What Are the Principles?
The collaborative process has produced six core principles:

1) Transparency
2) Dispute, Correction and Appeal
3) Accuracy and Validation
4) Model Governance
5) Independence
6) Confidentiality

The full description of each principle is available on the Chamber's website.

The Chamber's principles align closely with how we at RiskRecon describe our own solution capabilities:

- **Deep Transparency:** 50 unique security measurements derived from our proprietary analysis and complete vendor IT profiling and asset mapping.

- **Accurate Evidence**: all measurements result from our own direct, primary measurements of vulnerabilities, resulting in false positive rates under 1%.

- **Actionable Insights**: not simply ratings but direct measurements, supporting evidence, insights, and recommended actions.

- **Continuous Collaboration**: easily share our full assessment with your vendor without any time limits, vendor access fees, or other data constraints.

Regardless which solutions provider you choose for your security ratings, we agree with the Chamber that "to maximize their utility, both consumers of security ratings and rated companies need to have confidence that ratings are based on actionable, relevant information evaluated through a clear, articulable algorithm or data-driven process."

 © RiskRecon, Inc., 2018. All rights reserved.

Chapter 4: Security Vulnerabilities Don't Equal Security Risk – So How Do You Prioritize?

While security vulnerabilities are found in many technologies, their presence doesn't necessarily equal risk. Borrowing the FAIR Institute's definition, risk is the probable frequency and magnitude of loss. Knowing what security vulnerabilities are present in your infrastructure can help you understand the probable frequency, but it offers no indication of loss magnitude. Rather, solving risk requires two foundational data points: what security vulnerabilities your technology has, and the value of the assets in which those vulnerabilities exist. Without that context, a given vulnerability is the same as any other.

To illustrate, let's look at two remediation scenarios:

Scenario 1: Risk Analysis of 2 Vulnerabilities
Consider the threat of domain hijacking. Assume you have two domains: exampledomain.com and exampledomain.stinks. Both are missing the domain setting clientTransferProhibited that helps prevent domain hijacking. Which vulnerability is the higher risk? Additional context is needed to differentiate and prioritize. Exampledomain.com is used to host high-value web properties including an online banking portal; whereas exampledomain.stinks is a near-zero value asset that's been defensively registered to prevent malcontents from smearing the company's reputation. This context makes clear that exampledomain.com presents the greater risk.

Scenario 2: Risk Analysis of 32,829 Vulnerabilities
Yes, this is a real number. RiskRecon continuously assesses and monitors the information risk performance of thousands of companies; we discovered 32,829 issues in the internet-facing systems of just one of them. With so many, which ones represent the highest risk? Which ones don't matter? Why? This assessment is the heart of risk analysis. We can use issue severity and asset value to help:

Issue Severity
Opening 32,829 trouble tickets is simply a non-starter. So how do you prioritize? A practical starting point is to consult the vulnerability CVSS ratings provided through the MITRE-operated

Common Vulnerabilities and Exposures program. The CVSS ratings directionally inform us of the severity of each vulnerability, a key part of the risk equation.

CVSS Rating	Vulnerability Count
Critical	712
High	575
Medium	30,145
Low	815

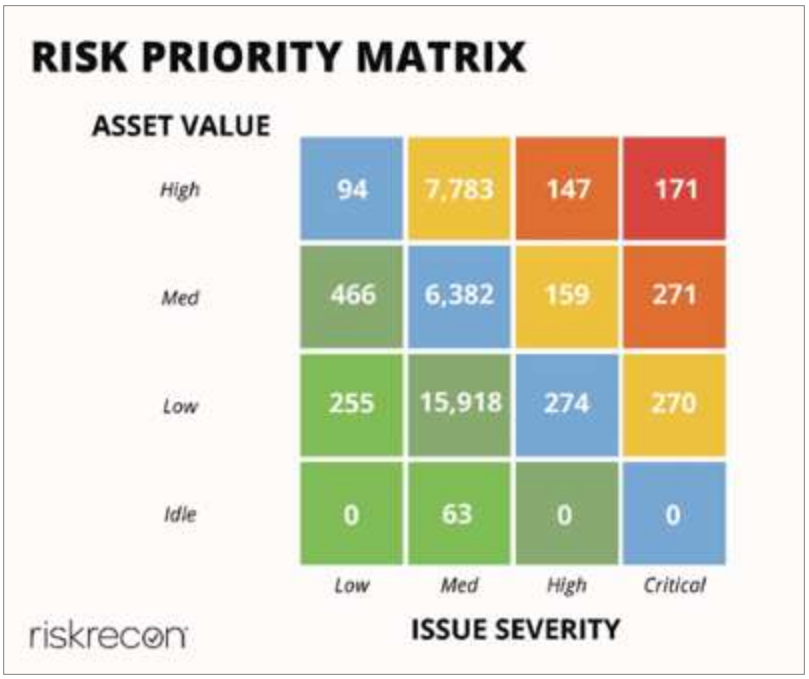
CVSS rating information is helpful. You can readily see the Critical and High severity vulnerabilities to address. It's also pretty safe to ignore those that are Low severity. But with 30,145 Medium severity issues, some of those will definitely matter. But which ones?

Asset Value

The CVSS rating information gets us at best half-way through the risk equation: understanding issue severity. Let's go ahead and add asset value using the following rating scheme:

1) **High-value assets** are transaction portals that require authentication to access or that collect non-public information such as tax IDs and email addresses;
2) **Medium-value assets** are systems that are brochureware sites, but that are network neighbors to high-value assets;
3) **Low-value assets** are systems that are brochureware sites that are not network neighbors to high-value assets;
4) **Idle value assets** are simply parked domains.

By adding asset value context to the assessment, we get a much more useful prioritization of issues based on actual risk. The visualization provides a ready roadmap for action via a Risk Priority Matrix:



The issues in the top right of the matrix stand out; those 171 critical vulnerabilities that exist in high-value assets (the red box). Once those are addressed, we'd likely pursue the 147 high-severity vulnerabilities in high-value assets and the 271 critical-severity vulnerabilities in medium-value assets (the orange boxes). Importantly, we also know what not to pursue: the nearly 17,000 issues in the lower left part of the matrix that represent low-severity vulnerabilities in low-value assets (the green boxes).

Chapter 5: What is the True Cost of Administering Your Vendor Security Questionnaire?

The more questions you ask in your third-party assessments, the higher the cost. But how much does an extra question really cost? And what is its value? In late 2017, RiskRecon explored this issue as part of a detailed study in which we analyzed the third-party cyber risk management practices of thirty firms. Let's walk through a few of the study data points that led us to the answer.

We asked our respondents how many cyber-risk relationships each analyst at their firm manages. The answer varied by sector; for example, Finance and Insurance companies assigned 73 vendors per analyst, Healthcare firms assigned 93 vendors per analyst, while Technology companies assigned 133 vendors per analyst—a big difference.

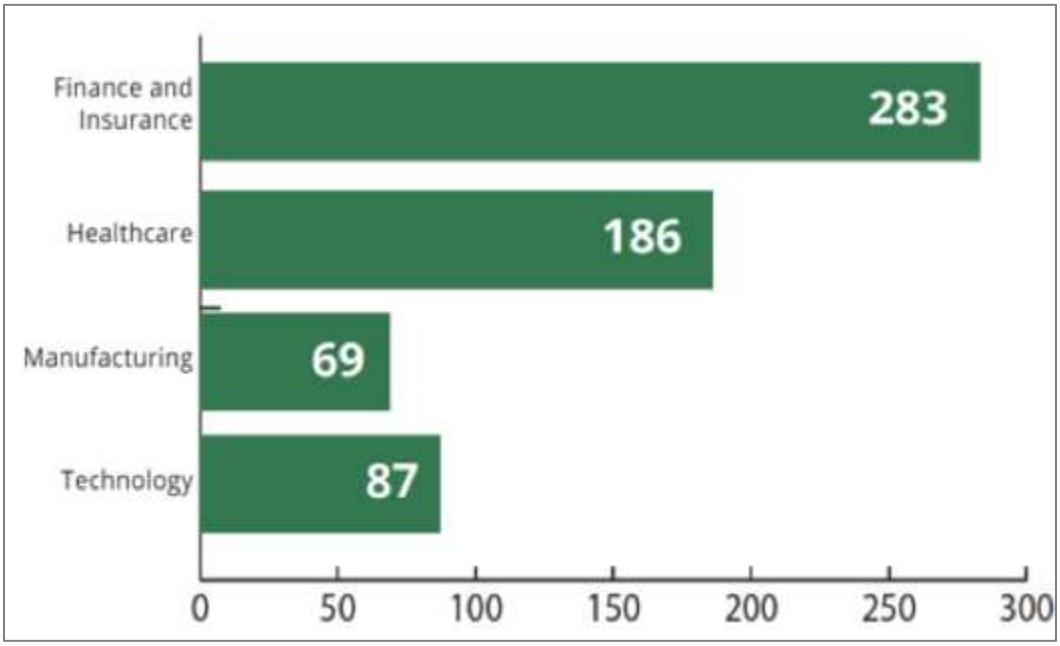
Figure 1: Number of third-party cyber risk relationship managed per analyst:

	Low	High	Average
Finance / Insurance	20	150	73
Healthcare	40	125	93
Manufacturing	32	175	102
Technology	67	200	133

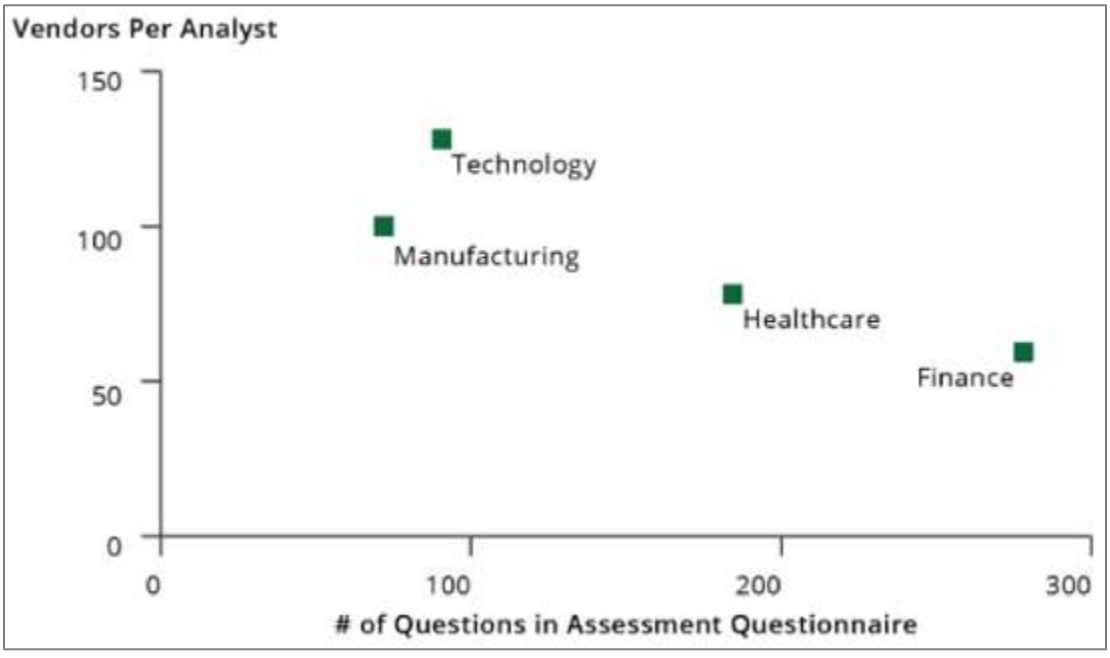
We also asked how many questions each respondent company had in their third-party assessment questionnaire. Finance and Insurance asked a whopping average of 283; Healthcare asked 186, while Manufacturing and Technology were both under 100 questions.

 © RiskRecon, Inc., 2018. All rights reserved.

Figure 2: Number of questions asked in the assessment questionnaire:



Combining the two data sets, we can clearly see that there is an inverse relationship between the number of questions in the questionnaire and the number of vendor relationships an analyst can manage.



The Cost per Question

It turns out that vendor questionnaires have some pretty decent economies of scale—the more questions you ask, the lower the cost per question. To project that cost, we have to extend our data set with a couple of safe assumptions. First, assume the fully loaded cost of an analyst is $120,000 per year. Second, assume each vendor is assessed on average every two years. On a cost-per-vendor-assessed basis, Finance is inefficient relative to other sectors. However, on a cost-per-question basis, Finance is actually much more efficient.

	Finance	Healthcare	Technology	Manufacturing
# of assessment questions	283	186	87	69
# of vendors managed / analyst	73	93	133	102
# of vendors assessed / year / analyst	36.5	46.5	66.5	51
Fully-loaded analyst cost / year	$120,000	$120,000	$120,000	$120,000
Cost per question	$11.62	$13.87	$20.75	$34.00
Cost per assessment	$3,288	$2,579	$1,805	$2,346

These are modest numbers. In practicality, the fixed cost of initiating the questionnaire is the most expensive aspect of the survey effort. Then there is a small marginal cost to each incremental question. But questions aren't really the point, are they? Good risk outcomes are the point. In your vendor questionnaires, ask only the questions that you must, but do ask them. Their value can be significant.

Consider the old adage that for want of a ten cent part, the bigger system was lost. As your data is entrusted to more and more external parties, increasing the rigor—such as asking the questions that need to be asked—of your compliance instruments just makes good dollars and sense.

Chapter 6: Why the Security of Your Vendor's Entire Enterprise Matters

Reliably protecting systems and data over time requires the disciplined execution of a robust security program that spans an entire enterprise. We've seen some vendors take the contrary position, arguing that customers need only be concerned with security of the systems that host their data.

Rarely can risk be contained to one set of systems and not be impacted by the threats and vulnerabilities of the surrounding systems and people. Grounding your third-party assessments in a correct, practical understanding of the cyber threat landscape will compel you to be concerned with your vendor's complete enterprise cyber risk management program, and not just the systems that you use.

Let's look at three points to consider when faced with a vendor's "contained risk" argument:

1) **Data that can be moved will be moved.**
On paper, most application stacks are well-bounded, supporting the argument that risk is contained to a limited scope. In this perfect world, your data resides in a database, data processing functionality is implemented in an application tier, and presentation logic is fulfilled through a web server layer. Backups may go to encrypted tape or to a remote network archive.

In imperfect reality, data does not just sit in a database. It takes a tremendous and rarely achieved level of organizational discipline and architectural investment to guarantee that data cannot leave its primary systems. If data can be extracted from those systems, it *will* be:

- Data is written to logging servers
- Analysts pull data from the database for analytics and reporting
- Network and server logs contain sensitive information
- DBAs query subsets of data in the process of supporting databases
- Production data may be used in test or QA systems

A compromise of any of these systems can result in compromise of your data. For example, in early May, Twitter advised its 330 million users to immediately change their

 © RiskRecon, Inc., 2018. All rights reserved.

passwords; it turns out that their password-hashing algorithm was writing the passwords in plaintext to a log server.

2) Systems are networked, facilitating unexpected attack paths.
The systems that store your data are interconnected with other systems. In most environments, it's pretty easy to construct an attack path against a "secure" environment that starts with compromise of an "out-of-scope" workstation or server. At a minimum, administrators, analysts, monitoring systems, back-up servers, remote access servers, and related web and application servers can directly access systems that store your data. These systems in turn are connected to other systems. A compromise of any system within the network path can result in compromise of other networked assets.

Consider the Equifax breach reported in September of 2017. Miscreants exploited an Apache Struts vulnerability on a consumer portal to gain initial access, then expanded into other systems. During his Congressional testimony, former CEO Richard Smith described the difficulty in conducting forensic analysis because of the sheer number of systems compromised. Equifax' admissions of exposed data have expanded since the breach was initially reported.

The 2011 breach of RSA offers another example. Hackers used spear phishing to compromise the system of a junior-level RSA worker who was outside of the expected attack profile, then pivoted across the organization until they reached a file server containing SecurID token seed values.

3) Lack of enterprise-wide security discipline will bite you in the end. All too often we've heard third-party CISOs and security professionals argue that severely vulnerable internet-facing systems don't matter because they are "low risk" and are unrelated to the customer environment. But ask yourself—do you trust an organization that spends more energy justifying operation of vulnerable online systems than just fixing the issue?

Third-party cyber risk management is ultimately about trust. Do you trust that moment-to-moment, day-in and day-out, your vendors will reliably protect your risk interests? Do you trust a vendor that has a 10 percent internet system software patching failure rate? Do you trust a vendor that only focuses threat intelligence operations on some internet points of presence but not others?

It may be that the systems hosting your data are patched, but vulnerabilities in other systems could be exploited to attack those where your data resides. If the vendor performs poorly as an enterprise, eventually that poor performance will show up in systems relevant to you.

Be very cautious of vendors who contend that their larger enterprise security program is none of your concern. That very argument demonstrates a lack of understanding of the cyber threat landscape. As Geoff Belknap, CISO of Slack put it, “If your business makes money by collecting, hosting or processing data from others, you’re a security company. Act like it.”

Chapter 7: Incorporating Continuous Monitoring into Your Third-Party Risk Program: Begin with the End State in Mind

Like many organizations today, you have existing processes, tools, and people laser-focused on analyzing periodic vendor security questionnaires, documentation, and on-site reviews. Moving to a continuous monitoring program can be daunting. Our advice: Don't focus on where to start…think about where you want to end up. Begin with the end state in mind.

Is today the day you say, "I'm ready"? Has the growing inherent risk associated with the number of vendors accessing your sensitive data finally convinced you of the need to do more than annual vendor surveys and assessments? Fantastic. The next question is, "where do I start?"

Many clients ask us how to get started. And I always respond by asking them about their desired end states. Meaning, what do they want their deliverables, metrics, and processes to look like in the future? And, can they articulate the most significant gaps in their current programs that they want to address and rectify?

Before you take that first step, let's review some things to help you determine your end goals. It's these end goals that will guide you as you incorporate continuous monitoring into your third-party risk management program.

When Thinking about Third Party Cyber Security, Keep Your End Goals in Mind
Generally speaking, organizations aim to move from a manual, one-size-fits-all vendor risk process to one that is scalable and risk-adjusted. Today, your vendor survey and risk process doesn't scale to effectively cover all third parties (and fourth parties) and doesn't obtain sufficiently frequent and actionable security performance metrics. Ultimately, you want a process that incorporates all vendors and suppliers and allows you to align assessment scope and frequency with your organization's residual risk tolerance and resources.

Determining what a risk-adjusted vendor risk management process means to your organization depends on risk appetite, potential exposure, budget constraints, system constraints, and other

 © RiskRecon, Inc., 2018. All rights reserved.

resource considerations. Therefore, when getting started, envision a risk-adjusted program that will answer these basic questions:

- **Who?** Which categories of vendors, suppliers, and fourth parties require coverage or more frequent coverage?
- **What?** Do you need separate processes for managed vendors, unmanaged suppliers, fourth parties, or vendors during the proposal process?
- **When?** How frequently do you require updated information for each category?
- **Where?** Into which steps in your process is it best to incorporate this new vendor risk data? Where do you want to remove, enhance, or streamline steps?
- **Why?** Do your defined metrics capture and assess the reasons behind this change? For example, have you established measurements to capture the number of additional vendors under coverage, increased frequency of coverage, and analyst productivity improvements?

Getting Started with Your Online Risk Assessment

Jumpstart your program by conducting a 90- to 180-day pilot with a set of vendors already scheduled for their annual assessment during the pilot period. During the pilot, build out your process according to the end goals you established:

- Obtain executive support to build an ad hoc team including security, sourcing, and third-party risk personnel. It's this team that will meet regularly, agree on key objectives and metrics, and help to evangelize the new continuous monitoring program throughout the rest of the organization.
- Establish the key pilot objectives and metrics, including impact on risk data quality and analyst productivity, remediation effectiveness, and third-party feedback.
- Select a third-party risk management provider that can provide continuous monitoring of all your third parties.
- Train your analysts on the new continuous risk scoring data, documenting how to build this data into your vendor engagement model. Shadow your analysts to determine what worked, or didn't work, during this initial phase and capture that feedback as well as any feedback from the vendors assessed.
- Meanwhile, gather an authoritative list of additional vendors not currently under review by your security team. Have your third-party risk management solution begin building portfolio and vendor-level risk assessments to prioritize which vendors to engage in phase 2 of your continuous monitoring project.

Chapter 8: Incorporating Continuous Monitoring into Your Third-Party Risk Management Program: The Pilot is Complete–Now What?

One of the most common questions we're asked is how to incorporate continuous monitoring into a third-party risk management program. In the last chapter, we discussed beginning with the end state in mind to establish goals for your continuous monitoring program and suggested you jumpstart your program with a pilot. So once the pilot is complete, now what?

Making Your Risk Management Software Work for You

The wheels are in motion. You've developed a reasonably good understanding of how to incorporate your new continuous risk assessment solution into your process, and have portfolio-level understanding of your vendor risks. Now, you want to take what you learned from the pilot and expand and mature your risk-adjusted vendor management model. And, you want to begin tracking suppliers and fourth parties that are currently unmanaged.

Your next step is to roll out the continuous risk assessment process and monitoring solution to your remaining managed vendors. Begin by engaging these vendors as their annual assessments occur, and establish thresholds in your monitoring program that alert you if a vendor deviates materially in between assessment periods. Over time, this historical monitoring information will help you establish a baseline of trust for each vendor. In addition, you should continue to add unmanaged suppliers and fourth parties to your continuous monitoring process.

Meanwhile, if you have not already done so, begin leveraging the objective, third-party data reports into your RFP process. You now have a rapid and actionable way to assess vendors during the proposal process (before they are contracted with) to help in the selection and to identify potential risks.

Your assessment provider's continuous monitoring and alerting capabilities should be integrated into your incident response process so that you can easily identify material changes that occur in between the standard assessment process. And when "celebrity vulnerabilities"

emerge, leverage the capabilities of your continuous monitoring provider to identify the specific third parties and systems exposed to this new threat. You will likely need to partner with your security and vulnerability management peers who may own or assist with investigation and response.

Continuous Improvement is Essential in Vendor Risk Management

With the passage of time, you will accumulate historical data on all managed vendors. And with the help of your assessment provider, you should also accumulate risk assessments for your unmanaged vendors and fourth parties. These assessments give you the necessary information to prioritize, in terms of size and scope, the inherent risk and historical quality of each vendor's security practices.

As our clients accumulate sufficient historical evidence, they typically find many ways to develop more productivity and control in their process:

- Receiving actionable information allows each analyst to cover more vendors as they spend less time preparing for assessments and can quickly pinpoint where to focus their efforts.
- Using historical risk and objective data already known about each vendor permits risk-adjusted frequency of the survey and attestation process.
- Similarly, clients can tailor the number of steps and overall assessment scope with the information provided by their continuous monitoring program.

The journey from kick-off to full implementation of your continuous monitoring program typically takes place over a year or more. As a result of that implementation period, you will have a risk-adjusted program informed by verifiable and objective risk assessment information. You will also be able to leverage historical trending information, consistent scoring, and actionable security alerts. This information and these capabilities will allow you to better scale your program, increase vendor coverage, and improve your control effectiveness.

About RiskRecon

RiskRecon's continuous monitoring solution delivers risk-prioritized action plans that enable precise, efficient elimination of companies' most critical third-party security gaps. Its data-driven SaaS service relies on passive, direct analysis of Internet-facing systems to quantify risks and provide straightforward evidence necessary for remediation. Rather than producing a laundry list of issues, RiskRecon's custom analytics quantify true risk by determining each system's issue severity and asset value. Only RiskRecon enables customers to build a scalable, third-party risk reduction program that compresses remediation cycle time, improves analyst productivity, and ensures constructive vendor collaboration. Learn more at https://www.riskrecon.com.

How to Get in Touch:

- Call us at (801) 758-0560
- Email us at sales@riskrecon.com
- Visit us on the web at https://www.riskrecon.com
- Request a demo at https://www.riskrecon.com/contact-us-demo.html

The material furnished in this document is believed to accurate and reliable. However, no responsibility is assumed by RiskRecon, Inc. for the use of this document or any material included herein.

RiskRecon, Inc. reserves the right to make changes to this document or any material included herein at any time and without notice. © RiskRecon, Inc. 2018. All rights reserved.