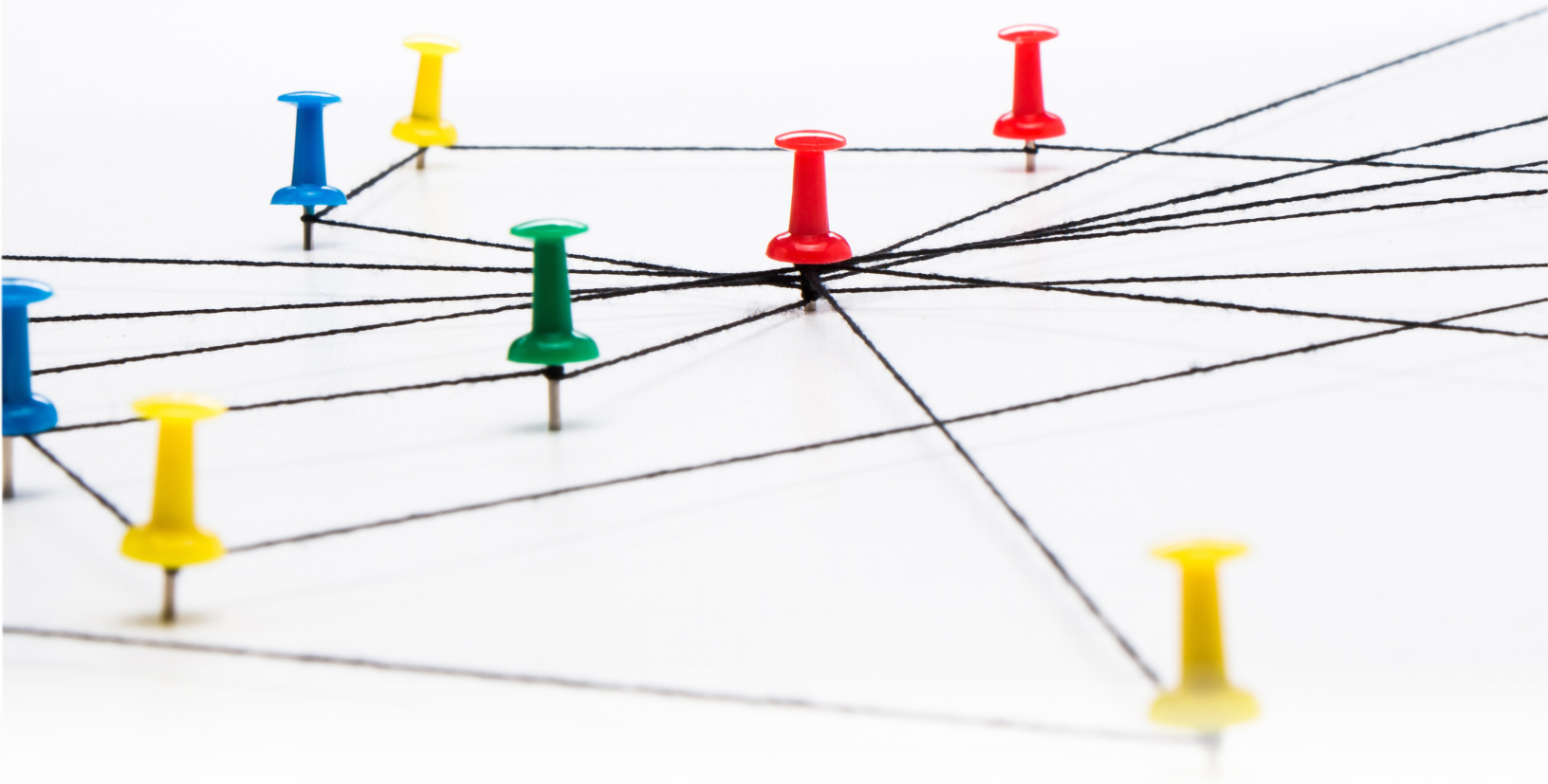
BITSIGHT®
The Standard in SECURITY RATINGS

How to Create a Scalable & Sustainable Vendor Risk Management Program

BITSIGHT®



Introduction

It's the prevailing economic narrative of our times: businesses are becoming more connected, more interdependent, and more global. Thanks to modern networking, companies are closer to their consumers, their clients, their investors, and their vendors than ever before.

To demonstrate this concept, picture your company as a pushpin on a cork board, connected with string to every third party that helps you operate. Materials suppliers, IT consultants, payroll processors, software providers…one pin for each of the hundreds, thousands, or tens of thousands of vendors in your network.

Now imagine all of those pins connected by string to each of their vendors. Zoom out, and you'll see a map of the entire global economy, with each business linked to an ecosystem of exponentially multiplying others.

This increasing interconnectedness shows no signs of slowing. According to Forrester, over 40% of global business leaders believe their firms experienced meaningful increases in Third Party dependence over the past year.

40%

Share of business leaders who believe their firms are increasingly dependent on third parties.

Source: Forrester October 20, 2017

This reality has a profound effect on risk in every form — reputational, financial, strategic, operational...the list goes on. This isn't news. In response to these risks, most businesses implemented vendor risk management (VRM) programs long ago.

However, when considering Third Party risk, one concern now stands apart from the others: cybersecurity.

Massive cyberattacks are routinely attributed to vendors with substandard security practices, and many of the victims of these breaches had existing VRM programs at the time they were attacked. As these data breaches become increasingly disastrous and IT regulations become increasingly strict, Third Party risk has taken on new meaning.

As a result, business leaders are losing faith in their existing VRM initiatives. Deloitte reports that 83% of them lack confidence in Third Party risk management processes. All of this points to one conclusion: traditional VRM processes and methods are no match for the realities of the modern vendor risk landscape.

In this Ebook, we'll explore those traditional programs and identify the areas where they fall short. We'll discuss what it takes to create a VRM program that's ready and able to stand up to the current state of affairs. Finally, we'll detail a step-by-step guide for creating a sustainable and scalable vendor risk management program from the ground up.

PART I: OUT WITH THE OLD

You might call them "traditional" or "legacy" VRM programs. Many were created prior to the emergence of cybersecurity as the leading Third Party threat, and now they're struggling to keep up. Despite their ineffectiveness, these programs continue to operate in the offices of the world's largest and most vulnerable companies.

What Does a Traditional Third Party Risk Program Look Like?

For traditional vendor risk managers, the assessment method of choice is the questionnaire. These extensive documents are sent to vendors, who, after some time, begrudgingly fill them out. Then the vendors send them back to the VRM department, who, after some more time, score them to determine the vendor's security posture. Because both vendors and VRM departments have limited resources, these questionnaires are completed infrequently, with months or years elapsing between each assessment.

Ideally, questionnaires would be highly customized for each vendor based on their company structure, the services they render, and the data they have access to within the risk manager's organization. Unfortunately, true customization is rare, and aside from surface-level changes, questionnaires often end up being a one-size-fits-all enterprise.

In order to verify the accuracy of the questionnaire, the vendor risk management personnel conduct some additional assessments. Typically, these consist of scheduled penetration tests and sporadic visits to the vendor's office to examine security controls in person.

These processes are almost 100% manual, and that has two key consequences:

First, the work has to be done by a dedicated VRM group, and it consumes all of their time. When a business scales up, resources must be added to the VRM department, or else the comprehensiveness of each VRM assessment must be scaled back.

Ideally, questionnaires would be highly customized for each vendor based on their company structure, the services they render, and the data they have access to within the risk manager's organization.

Second, the manual nature of the process lets in a certain amount of subjectivity. Because each vendor is so different, there is rarely a standardized policy for how much risk is acceptable. It falls to the vendor risk manager to make a judgement — a judgement which can be colored by a wide range of potential biases.

How Traditional VRM Programs Fit Within the Organization

How did it get to be this way? It all goes back to the context in which the VRM program was initially created, and the priorities of the organization as a whole.

In many industries, VRM programs were established as compliance-driven departments. In these cases, the job of the vendor risk manager was to ensure vendors had proper security controls and policies primarily so that the company could remain compliant with relevant regulations.

However, vendor risk is no longer just a subcategory of regulatory risk. Regulations typically dictate a minimum acceptable level of Third Party security. At the time these regulations were created, minimum acceptable security probably still wasn't enough to stop the most advanced cyber criminals. In the time since, the extremely dynamic cybersecurity landscape has rapidly outrun the effectiveness of these regulations.

In addition, legacy vendor risk management programs tend to be very siloed. Many of these programs represent just one small step in the vendor procurement process, and don't get much of a say in what happens before or after an assignment hits their desk.

While other departments have officers in the C-suite or a direct line to the Board, VRM programs have traditionally been given short shrift by executives. In the eyes of some leadership teams, VRM doesn't have a strong role to play in achieving key business objectives, and therefore is not worth the amount of time and energy they give to, say, legal, IT, or enterprise risk.

From a financial perspective, traditional VRM programs tend to be seen as a cost center. Because they are not aligned with greater business goals, it's easy to write them off as a necessary evil, a team that has to be kept around in order to meet regulatory requirements, but certainly not one that deserves additional resource allocation.

Why Traditional Vendor Risk Programs Don't Work

Questionnaires are only a point-in-time exercise.

The questionnaire, when combined with more advanced and objective risk assessment tools, can be a valuable resource for VRM personnel. When it's used as the primary solution, however, it can leave new risk unidentified and unaddressed.

Questionnaires are also time-consuming. Weeks might elapse between when a questionnaire is assigned and when it is evaluated. Completing questionnaires is a resource-intensive and sometimes unpleasant process for both vendors and VRM staff, leading to strained relationships and an uncooperative atmosphere.

Because the vendor is reporting on their own security posture, there is an opportunity for misinformation or inaccuracy. Even if the vendor does not intentionally lie, they could easily misunderstand a question, mistakenly check the wrong box, or have a lack of knowledge about their controls, policies, and procedures which translates, uncorrected, to the questionnaire.

In the time between assessments, a multitude of new cyber threats will emerge, and many of them will impact your vendors in some way.

Vendor risk managers then use these potentially flawed questionnaires to make important decisions, like whether a vendor should be allowed to continue accessing sensitive data, or whether the vendor relationship should be reevaluated entirely. These decisions are not always data-driven, and might vary from one manager to the next.

Traditional VRM methods can't keep up with the pace of cyber threats.

Questionnaires, pen tests, and site visits happen infrequently and are resource-intensive. In a large organization with thousands of vendors, it might not be possible to conduct these exercises frequently enough to reduce risk.

In the time between assessments, a multitude of new cyber threats will emerge, and many of them will impact your vendors in some way. According to Forrester, "Point-in-time risk assessments no longer provide the right data to conduct effective [third party risk management]."

These security "snapshots" are simply not enough in an extremely dynamic cybersecurity landscape. Even if we take them to be 100% accurate (which, as we've discussed, they rarely are), they will always offer an incomplete portrait of the risk a company is exposed to by a vendor.

The results of traditional VRM assessments are not actionable.

If a risk manager determines that a vendor does not have adequate cybersecurity, what happens next?

Because of the subjective nature of questionnaires and the sheer volume of data they represent, it can be extraordinarily difficult to pinpoint actionable information within their pages. What exactly does a vendor need to do to get up to snuff? How can the vendor risk manager prove that? What will happen if they don't improve?

Even if actionable information can be extracted from the assessment, VRM initiatives don't always have the teeth to force vendors into action. Either they report their findings to superiors who are too busy to do anything with them, or they report back to the vendor who may or may not take their suggestions.

In many organizations, it's not up the VRM team to decide which vendors stay and which ones go. In other words, third parties hold all the cards — without contractual obligation or pressure from leadership, they don't have a strong incentive to make changes.

In fact, because of the compliance-driven nature of traditional VRM programs, the principal duties of most VRM personnel involve identifying issues, not solving them. Their job is to meet the assessment requirements of various policies or regulations — following up on whether the results of those assessments are taken seriously by other departments is simply not part of their responsibilities.

PART II: IN WITH THE NEW

Solving the problems of legacy VRM programs requires a new way of thinking about Third Party risk. The solution requires buy-in from leadership, especially among GRC and IT teams. It requires new tools and new responsibilities for VRM personnel. Most importantly, it requires creating sustainability and scalability within the vendor risk management program.

VRM Revisited: A Perspective Shift

Many of the major issues that exist in traditional VRM programs can be traced back to the priorities of company leadership. If VRM is not considered a primary concern, it can't gain the resources and attention it needs to become truly effective.

Convincing the Board and C-suite to take vendor risk seriously doesn't require a huge leap of faith. Based on the latest surveys, it looks like most business leaders' understanding is already most of the way there.

According to the 2018 Allianz Risk Barometer, a major survey of global risk experts, business interruption is the most important risk today's businesses face. Among the the many causes of business interruption, cyber incidents ranked #1.

The only thing left to understand, then, is how likely it is that Third Party risk can lead directly to a cyber incident. One look at history can be enough to change minds on this front. Some of the most expensive data breaches in history, including news-making incidents like those at Target and Home Depot, were directly caused by poor security among vendors.

Third party risk doesn't just cause blockbuster data breaches, either. The scale at which this kind of attack occurs is staggering. According to Deloitte, 20.6% of business leaders report having dealt with a situation where sensitive customer data has been breached through third parties.

Once leadership understands just how real the risk of cyber attack via a vendor really is, it's time to use their buy-in to build a VRM program that's sustainable and scalable enough to address these risks.

Creating Sustainability

A sustainable vendor risk management program must have long-term goals and short-term objectives. It must have a steady and sufficient budget stream. It must also have procedures and policies that are robust enough to outlast any one individual.

More specifically, sustainability requires thorough integration into the larger organization, changes to the procurement process, and a solid level of agency and decision-making capabilities for VRM staff.

20.6%

Share of business leaders who experienced a data breach caused by third parties.

Source: Deloitte 2016

A sustainable vendor risk management program can't share the isolated positioning of its traditional predecessor. The leaders of VRM teams need to be integrated with other departments, especially legal, IT, security, and enterprise risk. This integration can take the form of increased collaboration, shared reporting, or shared resources.

In addition, VRM leaders should report directly to the C-suite and senior leadership on a regular basis. According to Deloitte, at "progressive organizations" "Third Party risk is starting to feature consistently on the Board agendas with CEO/Board-level responsibility." This level of executive engagement helps ensure that vendor risk management will continue to get the support it needs even as cyber risks and Third Party needs change.

Rethinking the way risk management plays into vendor procurement is also necessary if companies truly want to create sustainability. The VRM team needs to have their say in whether a potential vendor is a good fit for the organization before that vendor's products or services are purchased,

not after. In addition, the security posture of prospective vendors should be a primary consideration during the exploration, shortlisting, and selection phases of the procurement process.

Importantly, vendor procurement is also the time to give the VRM team the tools they need to enforce sustainable cybersecurity practices among the Third Party network. Good cybersecurity controls, policies, and procedures should be a contractual obligation, and these requirements should go above and beyond the requirements of regulatory authorities.

In a sustainable vendor risk management program, personnel must have the agency to communicate with and make decisions about third parties. In other words, the VRM team needs a channel to communicate with vendors and let them know about security issues. If the vendor does not agree to resolve these issues in a timely manner, the VRM team needs to have the ability, in cooperation with other departments, to make decisions about whether that vendor's products or services continue to be used.

Creating Scalability

Scalability and sustainability go hand-in-hand. In order for a VRM program to be truly sustainable, it has to be able to scale with business growth.

When it comes to vendor risk management, scalability means having the ability to manage thousands of vendors as effectively as you manage ten.

The traditional arsenal of VRM tools does not have the ability to scale quickly and effectively. Questionnaires, site visits, and pen tests produce “point-in-time” or “snapshot” assessments of vendors' cybersecurity posture. As detailed above, these assessments are completed far too infrequently to provide accurate and actionable information. These types of manual assessments also require an expenditure of resources that is extremely likely to become a roadblock to scale.

Thankfully, there are solutions available that allow VRM teams to assess and monitor their Third Party risk continuously.

Over the last few years, security ratings have changed the way vendor risk management teams operate. A security rating provides an at-a-glance look at the cybersecurity posture of any given company. These ratings are collected through an objective, automated process. Most importantly, they are updated daily.

BITSIGHT

Quality security ratings, like those provided by BitSight, have been proven to directly correlate to the likelihood of data breach at a given organization. The lower the rating, the more concerned you need to be about your data.

Companies with a BitSight Security Rating of 500 or lower are almost five times more likely to experience a data breach than those with a rating of 700 or more.

With security ratings, VRM professionals can assess their entire vendor landscape at once, instead of relying on "point-in-time" assessments. If a vendor's rating drops below a certain threshold, the VRM team is notified and can take appropriate action.

In addition, many security ratings providers allow customers to go beyond the overall rating and gain deeper insight. With these detailed reports, a company can see in exactly which areas a vendor's security is posing risk. Then, VRM teams can use this actionable information to communicate effectively with the vendor and arm them with data to resolve issues.

A vendor risk management team that uses security ratings might still use questionnaires, pen tests, and site visits. These processes are still valuable — they can reveal information about facets of security that security ratings don't have visibility into. However, by making them the secondary source of data rather than the primary one, VRM professionals are able to streamline their work and complete faster, more comprehensive assessments of more vendors.

All of this also equates to a reduced need for more resources as vendor bases grow and expand. In traditional vendor risk management programs, scaling up meant hiring additional staff. In modern programs, that's not necessarily the case.

A truly scalable VRM program needs to streamline more than assessment processes. Auxiliary processes, like communicating with vendors and with company leadership, must be streamlined as well.

With security ratings, VRM professionals can assess their entire vendor landscape at once, instead of relying on "point-in-time" assessments.

Some security ratings services like BitSight enable easy communication with vendors by giving them access to the security ratings platform. When vendors can see their riskiest areas for themselves, they can take quick action to fix the problem.

Security ratings are also indispensable for reporting. In the new setup of increased integration with other departments and increased time with the C-suite and Board, the importance of reporting becomes magnified. Being able to deliver quantifiable results about vendor risk will help a VRM program remain efficient and effective, and help businesses use VRM data to improve decision-making.

PART III: BUILDING A MODERN VRM PROGRAM

Here is a step-by-step guide for creating a sustainable and scalable vendor risk management program from the ground up.

1. Create the Foundation

Before you start assessing vendors, you must lay the groundwork for your VRM program. Make these decisions carefully — they will affect how your VRM initiatives operate for years to come.

First, you'll need to build a team. Ideally, the personnel you choose will bring a good mix of experience and knowledge to the table. With cybersecurity, risk, business, and legal know-how represented, your team will have the intelligence it needs be extremely effective.

At this stage, it's also important to develop internal policies regarding reporting and decision making. Who answers to whom? Who has the ability to make which decisions? Who is allowed to directly communicate with vendors? Who will report to the senior leadership, and how often?

You'll also need to develop a strict set of policies that govern acceptable levels of vendor risk. This will help remove subjectivity from the assessment and procurement processes.

Finally, you'll need to select the providers you'll use for automated vendor risk management solutions. Take the time to thoroughly research several security ratings solutions. This will likely be the last time you choose a provider without the assistance of a modern VRM team.

2. Discover Your Data

Once the VRM team is assembled and their policies are established, it's time to begin a comprehensive review of your organization's existing vendor landscape. During this process, you'll be identifying and examining vendors that have access to sensitive data.

Before you can do that, you'll need to decide what "sensitive data" means to your organization. For many, it simply means consumer data, personal identifying information, and credit card information. For others, "sensitive data" could include classified programs, intellectual property, or even trade secrets.

After you determine which data matters most, you need to discover where it lives. Many organizations are surprised to learn just how much of their sensitive information is being stored outside of their organization, in cloud servers or in the databases of vendors.

Next, compile a list of every vendor and the data they have access to. This will be a time-consuming process, but it will save you a significant amount of resources later on.

3. Prioritize Your Vendors

Once you've compiled a comprehensive list of vendors and determined what types of data they have access to, it's time to organize them based on the sensitivity of that data.

Unless you have an incredible amount of resources or an incredibly small roster of vendors, you're not going to be able to completely assess the risk of every third party your organization does business with. For this reason, it's important to prioritize them and identify the most critical relationships to be assessed first.

4. Assess Critical Vendors

Now that you've identified the vendors with access to your most sensitive data, it's time to perform some risk assessments.

Use a combination of techniques to assess these vendors' cybersecurity. Security ratings should be a primary assessment method, as they allow you to continuously monitor cybersecurity risk. However, questionnaires, penetration tests, and other assessments should also be utilized, especially for these critical third parties.

5. Engage with Existing Vendors

If during your assessments you find that some vendors are not performing up to the standards you set at the beginning of the process, it's time to communicate with them about resolving their outstanding security issues.

Security ratings are a great asset in this communication. They allow you to have data-driven, evidence-based conversations with vendors.

Sometimes, vendors are simply unaware that they weren't securing their data properly. In these cases, just making a vendor aware of specific issues can be enough to get them to commit to results.

In other cases, you'll need a little more leverage to get vendors to improve their security practices. If a vendor is slow to respond or seems unwilling to change, determine what you need to do to escalate the situation. Sometimes, this means reviewing or strengthening contractual obligations. If a vendor still refuses to change, you might need to find a replacement.

Finally, part of the responsibility of the VRM team is staying up-to-date on the latest cyber threats and vulnerabilities. When these arise, determine how they affect your vendors and your organization, and take appropriate action.

6. Procure New Vendors

Your vendor risk management team should be present and active throughout the procurement process. Security ratings should be used to inform the exploration, selection, and shortlisting processes.

Once you decide on a vendor with an acceptable security posture, make sure you build security performance requirements into that vendor's contract. Security ratings give you an opportunity to quantify and track this obligation. For example, you may write that if the vendors' BitSight security rating falls below 550, you have a right to terminate the contract.

BITSIGHT

CONCLUSION

For a variety of reasons, traditional vendor risk management programs are not effective at assessing and mitigating risk in ever-expanding Third Party networks. With the emergence of cybersecurity incidents as the greatest of these risks, this ineffectiveness leaves businesses vulnerable.

Luckily, services exist that can help VRM programs stand up to the realities of Third Party cybersecurity management. By implementing these services within a sustainable and scalable program, businesses can protect themselves from cyber threats and improve relationships with their vendors.

Want to take your VRM knowledge to the next level?

Take Control Of Vendor Risk Management Through Continuous Monitoring, a March 2018 study conducted by Forrester Consulting on behalf of BitSight, sheds light on the current approaches organizations are taking towards VRM.

ACCESS STUDY