BITSIGHT
The Standard in SECURITY RATINGS

WHITE PAPER

Faster, Less Costly, and More Scalable

Here's how your vendor onboarding program can have all three

Introduction

When onboarding new vendors, it takes the median company an average of 90 days to complete due diligence – 20 days longer than four years ago.

-Gartner[2]
Enable Value and Manage Risk Through Compendious Supplier Onboarding

Today's businesses cannot succeed on their own. That is why, according to Gartner, 60% of organizations now are working with more than 1,000 third-parties, including partners, sub-contractors, and suppliers.[1]

Companies work with these additional organizations to become leaner, more agile, flexible, and efficient, so they can go to market faster and beat the competition.

Bringing in new vendors requires a vigorous and extensive onboarding process to ensure they maintain an acceptable security posture and don't introduce unwanted risk. At the same time, a lengthy process undercuts businesses' efforts at digital transformation and growth acceleration, and impedes them from being able to maximize the value from their vendors.

In today's business climate, no one has time for a 90-day onboarding process.[2] Indeed, the act of onboarding vendors needs to match the velocity that the rest of the organization is trying to achieve.

Accelerating the onboarding process, however, can put pressure on you — the security manager — to evaluate all vendors in a consistent manner and complete security assessments quickly. But using a "one-size-fits-all" mentality to the onboarding process makes it unscalable, creates significant overhead, and fails to take into consideration the variances among different vendors. Rushing the due diligence process could also result in unacceptable or unknown levels of risk sneaking into your organization.

You need to find a balance between speed and security by implementing:

- An efficient onboarding process that supports the goals of your organization
- A scalable and adaptive process that prioritizes and assesses each vendor based on the relationship and access they have to your company
- A cost-effective approach that saves time and money, yet still maintains a high security standard

In this white paper, we will take a look at some of the challenges that keep today's vendor onboarding processes from supporting the needs of modern businesses. Then, we will explore how you can address those challenges by streamlining vendor onboarding in a way that makes your security team a good partner to the business — one that is in alignment with your organization's need for agility, flexibility, and scalability.

Pressure In The Onboarding Process

59%

of companies have experienced a data breach that originated from a third party.

-Opus/Ponemon[3]
Data Risk in the Third-Party Ecosystem: Third Annual Study

To start, let's acknowledge that the vendor onboarding process can be extremely tense and fraught with risk. In fact, it may be the most pressurized time during the client-vendor relationship, for a couple of reasons:

- **Pressure from leadership to onboard new vendors quickly**

  Executives want to increase agility and flexibility so they can build competitive advantages and drive innovation. Onboarding third-party vendors quickly can help them achieve these objectives. As a result, leadership puts pressure on functional business heads to accelerate the onboarding process.

  That pressure, in turn, is passed along to you. Under that pressure, you may feel forced to make quick decisions, with little or no time to perform a proper risk assessment. You even may feel compelled to cut corners — for instance, you may not do a thorough job, or elect to skip the assessment altogether. Or, you may take too long, only to have the business sign with the vendor anyway before the assessment is complete.

- **Pressure to oversee vendors and ensure that they are secure**

  Leadership expects the vetting process to be extremely thorough, and that third parties adhere to the company's security standards. In fact, according to Gartner, 65% of legal and compliance leaders report their boards and senior leadership demand increased oversight of third parties.[2]

  While you need to get contracts in place in a timelier manner, you also must ensure that the third parties you are bringing into the fold don't introduce unwanted or unknown risks. Yet, as the number of third-party vendors in your company's arsenal continues to grow, it becomes an enormous challenge to perform the proper due diligence before entering into a partnership, especially when costs begin to rise and time and resources are limited.

  To make sure your process is thorough, it can be all too easy to fall back on traditional methods or cookie-cutter approaches, making sure every last question and certification for every vendor is obtained.

  This "one-size-fits-all" approach is common for organizations that lack visibility into their vendors' security postures and do not have the necessary resources to know the level of risk for the vendor. While subjecting every vendor to the same assessments and security standards can be enticing to make sure you reduce risk, it can be more assessment than what is needed for many vendors, especially non-critical ones.

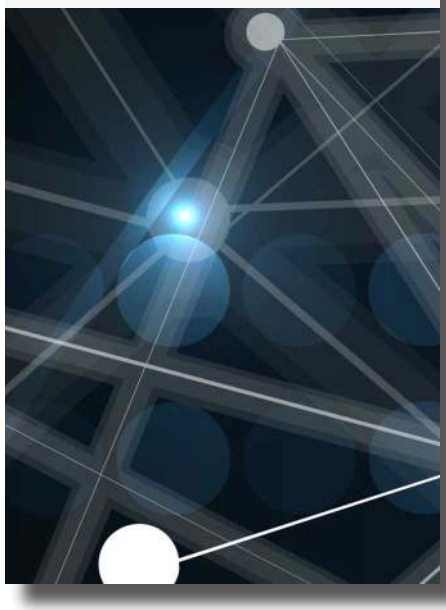
  It also can be a costly mistake.

No Two Vendors Are The Same

16%

of organizations say they effectively mitigate third-party risks.

-Opus/Ponemon[3]
Data Risk in the Third-Party Ecosystem: Third Annual Study



Different vendors present variable risk levels. A payroll provider working with sensitive employee and company information represents a much higher level of inherent risk and merits different treatment.

Treating all vendors the same as the payroll provider, however, creates issues related to time, resources, and scalability. You end up spending the same amount of time and money assessing every third-party vendor — using the same boilerplate questionnaires — no matter their size or risk potential. As such, your security assessments are not as customized, effective, or streamlined as they need to be.

It is a process that is static and non-scalable, making it hard to manage your already stretched resources effectively.

Furthermore, this approach also can lead to inaccurate assessments rife with incorrect information that could result in unknown risks to your business.

For instance, a smaller vendor may not have the time, resources, or cybersecurity know-how to give thoughtful, or even accurate, responses to a lengthy questionnaire with 1,600 inquiries. Instead, they may just "check the boxes," roughly piece it together, and call it good. They even could decide not to respond and pass on doing the assessment altogether, or turn in an incomplete questionnaire.

From your perspective, you may elect just to take a questionnaire at face value and not validate the responses — or, you may overcompensate by going in the opposite direction and perform on-site assessments or more in-depth evaluations. The former approach can result in unknown vulnerabilities entering your company, while the latter can be extraordinarily costly. Plus, it virtually is impossible to engage in this level of customization and detail if your organization is dealing with hundreds, if not thousands, of third-party vendors.

In the worst-case scenario, if you are under pressure from leadership to onboard third parties and unable to scale your assessments, you may opt to skip the entire due diligence process altogether.

Streamline Onboarding To Empower Your Business

> Not all vendors will have the same risk threshold. Group and prioritize vendors based on their criticality to your business or the type of data they will be handling.

Fortunately, it doesn't have to be this way. Instead, you can implement adaptive assessment processes that are efficient, thorough, and scalable. You can accelerate vendor onboarding to enable fast value creation without introducing unknown risk.

Let's look at three key strategies you can adopt today to onboard new vendors securely — at the speed of business.

1. **Prioritize your vendor analysis**

   Instead of looking at every vendor in the same manner, group and prioritize vendors based on their criticality to your business or the type of data they will be handling. Not all vendors will have the same risk threshold. You may grant a higher level of risk tolerance to less critical vendors that hold no data or do not have access to your corporation's network, versus a critical vendor that holds a great deal of data or maintains constant contact with your company's systems.

   For instance, non-critical vendors may not require a full questionnaire to be completed. Instead, you simply can focus on areas of risk and collect their certifications. This could, in and of itself, expedite the assessment process because you will be focusing your attention on specific areas of risk and not spending as much of your resources on a vendor that has less business impact.

   Meanwhile, the payroll provider may require a closer level of scrutiny than the food service operator. Perhaps the former is worthy of an in-person site visit or a more in-depth assessment.

   In the end, it's all about tailoring your onboarding process. Eliminating the one-size-fits-all mentality in favor of a customized and scalable approach improves agility and bolsters security.

2. **Define thresholds for acceptable levels of risk**

   Determine your acceptable risk thresholds and develop policies around these findings. Make sure that every potential vendor is assessed accordingly. Establish criteria both for the total risk posed by the vendor as well as the threat posed by individual factors of their security posture, such as unpatched systems, legacy and unsupported technologies, history of malware infections, and more.

   To make this work, establish a culture of cross-collaboration across various departments. Involve everyone from the CEO, the CIO, and the CFO to the head of legal in determining your organization's risk appetite — what is acceptable and what is not. Some of those leaders already may have created their own set of security policies that you can incorporate into your vendor onboarding processes.

   Know that the responsibility should not be yours alone. Security must be everyone's concern, particularly when it means bringing in an unknown third-party.

3. Develop contract language that makes thresholds and remediation enforceable

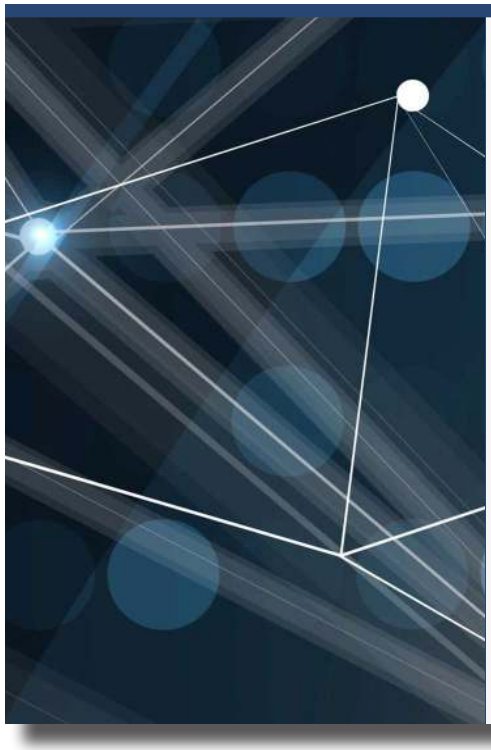
Work closely with your legal department to create contract language that guarantees your third parties will uphold their end of the security bargain.

Your contracts could stipulate that vendors will not fall below the agreed-upon risk thresholds and that they will employ ongoing security monitoring to ensure their compliance.

Include language that the vendor agrees to respond to your inquiries and notify you about breaches promptly, and spell out specific mandates and timelines for expeditious remediation.

This will require a common set of standards that are clear and easy to understand. External data sources, such as security ratings, are ideal for this purpose, and also can help you streamline your assessment processes.

Let's take a closer look.



Organizations with high levels of board engagement, and understanding of, vendor risk management (VRM) issues are more than twice as likely to have VRM programs that are operating at or above target level, compared with organizations that have low levels of board engagement in these issues.

-Shared Assessments Program and Proviti[4]
2019 Vendor Risk Management Benchmark Study
Running Hard to Stay in Place

Rate Your Vendors' Risk Level

Security ratings provide immediate, up-to-date data about a third party's security posture.

Similar to a credit score, they are used to assess a vendor's potential risk exposure and attribute a numerical value to their organization, with a higher number indicating a more secure environment. Security ratings provide details on a number of areas including vulnerabilities, unpatched systems, malware infections, insecure access points, and more.

Security rating data is useful to prescreen vendors during the evaluation, RFP, and procurement phases. You can glean insights into which potential partners need more in-depth assessments or even eliminate vendors from consideration altogether if they do not meet established risk thresholds.

You also can use the rating to optimize and prioritize your risk assessment strategies and potentially reduce the number of questions that are asked during the assessment. For example, if a vendor receives a high security rating, you may opt to forgo some of the common hard inquiries and reduce the number of questions you ask.

The assessment and onboarding phase is only the beginning. You also will need to ensure that your partners remain secure throughout the life cycle of your engagements.

Incidents attributed to hackers, competitors, and other outsiders have declined. However, those attributed to insiders, such as third parties – including suppliers, consultants, and contractors – have stayed about the same or increased.

-PwC[5]
The Global State of Information Security® Survey 2018

Implement Continuous Security After The Contract Is Signed

Unlike a questionnaire or onsite assessment that provide only a point-in-time snapshot of your vendor's security posture, security ratings are assessed continuously.

When the onboarding process is complete, it doesn't mean that your work is done.

Although you may have scheduled a reassessment, especially for your critical vendors, organizations must never lose visibility into the security posture of their vendors, critical or otherwise. Once you have entered into an agreement with your third party, it is important to implement continuous monitoring practices that provide assurance that the vendor is maintaining a good security posture.

Security ratings can do this in real time.

Unlike a point-in-time snapshot, security ratings are assessed continuously, and you can receive instant alerts whenever a vendor's rating falls below an agreed-upon threshold. This helps maintain the same high security standards established at the outset of the partnership.

Monitoring for ongoing issues across both critical and non-critical vendors also can help inform whether regularly scheduled assessments are required.

For example, continuous monitoring may reveal that a non-critical vendor is maintaining a healthy cybersecurity posture and no reassessment is needed at the scheduled time — saving time and resources. Meanwhile, if the security rating of a critical vendor begins to slip, it is an indication that a reassessment should be performed immediately.

With security ratings, you continually can verify, validate, and hold your vendors accountable for their security measures. You don't have to let all of the excellent work you have done in the onboarding phase be for naught.

Optimize Your Vendor Onboarding Process

Leadership expects the vendor onboarding process to match the speed at which their organizations are moving.

Vendors can play an important role in your business' drive for innovation, agility, and flexibility. As such, leadership expects the vendor onboarding process to match the speed at which their organizations are moving. They want it to enhance and empower — not inhibit — their corporate objectives.

That puts a lot of pressure on you to accelerate your onboarding processes and make them more efficient, scalable, and flexible — in short, more like the business itself. But you cannot afford to do this at the expense of performing the appropriate level of due diligence to avoid introducing risk into your organization.

Through the strategies we have outlined here, you can achieve all of these objectives without compromise. You can cut down on the time it takes to onboard partners from months to weeks or even days. You can reduce costs and deploy resources to areas that truly need them.

And you can move forward knowing that *all* of your third-party vendors — even if they number in the hundreds or thousands — present acceptable levels of risk to your organization.

REFERENCES

1 https://www.gartner.com/smarterwithgartner/a-better-way-to-manage-third-party-risk/

2 https://www.gartner.com/en/documents/3953452/enable-value-and-manage-risk-through-compendious-supplie

3 https://www.marketwatch.com/press-release/opus-ponemon-institute-announce-results-of-2018-third-party-data-risk-study-59-of-companies-experienced-a-third-party-data-breach-yet-only-16-say-they-effectively-mitigate-third-party-risks-2018-11-15

4 https://www.protiviti.com/US-en/insights/vendor-risk-management?utm_source=ProPress&utm_medium=Referral&utm_campaign=VRM+Survey

5 https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

BitSight Security Ratings deliver better data for better decisions about your organization's security.

Learn More.

www.BitSight.com

BITSIGHT
The Standard in SECURITY RATINGS

111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

About BitSight

BitSight transforms how organizations manage information cybersecurity risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to analyze vast amounts of data on security issues continuously. Seven of the top 10 largest cyber insurers, 25 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks. For more information, please visit www.BitSight.com, read our blog, or follow @BitSight on Twitter.