ULTIMATE GUIDE TO VENDOR RISK ASSESSMENT

whistic

ULTIMATE GUIDE TO VENDOR RISK ASSESSMENT

How to modernize your approach to vendor risk assessments

It wasn't that long ago that assessing third-party vendor risk wasn't much of a concern for InfoSec teams. Applications were hosted on-premise, meaning the business had total control over customer data and how it was secured. As a result, assessing a vendor's security posture frequently wouldn't even come up during the sales process.

But that all changed once businesses started shifting from on-premise to the cloud. According to a McKinsey & Company report, by 2024 one third of all enterprise software purchases will be SaaS[1]. This shift has put third party vendor security at a premium because businesses no longer have complete control over the security of the data belonging to them and their customers.

Businesses invest a lot of time and money securing data under their control, but if they allow an unsecure vendor into their environment, all that effort would be for naught. In fact, data breaches that involve a third party vendor are more costly than other types of breaches, costing businesses $4.29M on average and take nearly 300 days to identify and contain[2]. However, the ongoing effects, such as loss of trust, last years beyond the initial breach.

And despite everyone's best efforts, no one is immune to a data breach. Data from IBM shows that the probability a business will experience a breach within the next two years is 29.6%[3]. To mitigate the risk of a breach, it is suggested that businesses should adopt risk management and compliance programs, which include security assessments and audits[4].

Although SaaS sales teams and their customers and prospects know they must address security before deals can get done and solutions are implemented, doing so can cause unwanted delays in the sales and buying process. That's because as threats have evolved and become more sophisticated over time, the tools and processes for managing and assessing vendor risk —typically spreadsheets and email—have stayed the same.

Recent advancements have made it possible for SaaS vendors and buyers to streamline and modernize how vendor assessments are handled, easing the burden on overworked security teams and speeding up the process for buyers and sellers alike.

This ebook highlights four steps both buyers and sellers should follow to improve the process for assessing a vendor and responding to questionnaires with the ultimate goal to protect valuable customer data. The steps include:

1. **Rely on standardized assessments when you can**
2. **Be transparent**
3. **Take a proactive approach to vendor security assessments**
4. **Centralize the management of vendor security assessments**

The cost of data breaches involving a third party vendor.

$4.29M

1

Rely on standardized assessments when you can

One of the biggest headaches InfoSec teams deal with when responding to security questionnaires is the sheer amount of time it takes to fill them out.

This is because there isn't a consensus on which questionnaire should be used, and as a result, most questionnaires, 71% according to RiskRecon[5], are custom, many of which have hundreds of questions.

The trend for industries to adopt a standardized set of questions is picking up momentum but will still take years to fully occur. Until that time comes, it is recommended to utilize standard questionnaires whenever possible. While every business is different and may require some additional questions and follow up, most security concerns can be addressed by one of the many standard questionnaires available to you.

Relying on standard questionnaires means responses will likely be faster, resulting in shorter buying and selling cycles and the ability for teams to utilize critical applications needed to run your business sooner rather than later. Because there are so many questionnaires available, it can be difficult to know which one will be best for your business. To help, we've outlined a few things to consider when making your decision along with a brief primer on some of the more popular questionnaires.

Things to consider

How experienced are you with vendor security assessments?

Whether you have a robust program to assess third party risk or you're just getting started there's a questionnaire for you.

Where are your business and customers located?

There are laws in some countries or states that require you to meet certain security standards to handle private customer data.

What's your industry?

While not every industry has a questionnaire dedicated to them, some like higher education or government, for example, do.

Are you working toward a particular certification or compliance standard?

Some questionnaires are helpful and necessary when you're working toward earning security certifications or trying to achieve compliance in certain areas.

Tips for security questionnaires

It's no secret that responding to questionnaires can be tedious and time consuming, but if you follow these tips the process should improve greatly.

Build out a library of answers

While each questionnaire might be different, that doesn't mean the answers from one won't be relevant and applicable to another. Having a library of answers in place will help you respond to questionnaires more quickly and efficiently.

Save and reuse standard questionnaires

One of the biggest benefits of adopting standardized questionnaires is they can be used over and over again with minimal editing, saving the InfoSec team time they can use to focus on mitigating risk as opposed to completing administrative tasks.

Keep your security certifications up-to-date

A surefire way to quickly build trust with a prospect is by including current security certifications with your questionnaires to show how deep your commitment to security is.

Utilize technology to streamline the process

With the large number of vendor assessments most businesses have to manage, spreadsheets just won't cut it anymore. Utilizing a platform that enables you to quickly build a security profile that can be utilized over and over again is a must have for teams that strive to be more efficient.

2

Be transparent

Transparency is the key to building trust with your customers, especially when it comes to your security and risk posture. Not being forthright and honest from the beginning can slow deals down or even cause you to lose them outright.

When asked about the characteristics of best-in-class SaaS vendors on security, 70% of respondents in a McKinsey & Company survey cited transparency[6]. That same study also found that more than 70% of respondents said uninformed or misleading claims about security capabilities were a cause of dissatisfaction[7].

Vendor security assessments are a good place to forge transparent relationships with your customers. They allow you to be upfront and straightforward about the security practices you have in place to ensure privacy and protect customer data. Having an issue with your security assessment is a surefire way to disqualify your business from consideration.

70% of cyber professionals cited transparency as a characteristic of best-in-class vendors on security.

Tips for Transparency in Security Reviews

There are a lot of little things your business can do to show your customers that transparency about your security practices and policies is a priority for your business. A few are highlighted below.

Make your security profile public

Having a public profile posted on your website, in a directory like the Cloud Security Alliance's STAR Registry, or in the Whistic Trust Catalog, that your customers and prospects can access quickly and easily shows that you have nothing to hide. While there may be some details about your security posture that you'd prefer to keep private, a public profile oftentimes provides enough information to pass a security assessment.

Be responsive to questions and concerns

Once a prospect has reviewed your security profile or response to an assessment, they may have additional questions or need more clarity. Respond to these requests quickly with precise, thoughtful answers. Make sure everything you say can be backed up and doesn't mislead the customer about what your security capabilities are.

Actions speak louder than words

Being fully transparent with your customers can be hard, especially if there are current limitations in the security of your solution. But your customers will appreciate understanding the true picture and will oftentimes engage with you to address gaps that might prevent them from doing business with you.

3

Take a proactive approach to security reviews

It's no secret that responding to vendor security assessments can be a headache, and that could be why SaaS sales teams often put them off as long as possible. But doing so most likely will push deals out.

In fact, according to research by Gartner, addressing security concerns is the most-cited cause for delay in technology buying decisions[8]. That's why the most successful sales teams take a proactive approach when it comes to vendor security.

There are a couple of tactics you can implement that will not only help you close deals faster, but also set yourself apart from the competition by using your security posture as a competitive advantage.

65% of technology buyers say addressing security concerns caused delays in technology buying decisions.

Share your security profile

The first step in taking a proactive approach to security reviews is sharing your security profile, including standard questionnaires and certifications, early in the sales process. This helps build trust with customers and prospects from the outset of your relationship. It could also mitigate lengthy back and forths that often occur during the security review process because you answered their questions ahead of time.

To ensure your profile is sent at the right time in the sales cycle, you can build it as part of your standard sales motion through your CRM. Automating the process means that security questionnaires never slip through the cracks.

Proactive security reviews in action

One company who has taken this proactive approach to vendor security to heart is Gremlin[9], a leading Chaos Engineering platform, but that wasn't always the case.

In the past, their InfoSec team may not have been engaged until a few weeks before the deal was supposed to close. The rush to fulfill these requests, while also staying on top of their other day-to-day responsibilities, proved difficult.

It also caused significant delays in their sales cycles. It would take the team 45–60 days on average to complete one security review. Over time the problem grew to the point where they were having to respond to over 100 security reviews every few months. It didn't make sense for them to continue answering the same questions over and over again.

To solve this problem, they implemented a solution that would allow them to put together a profile that leveraged previously completed questionnaires along with all of their supporting documentation and their sales team started sharing this security information early in the process. Since shifting to a proactive approach, Gremlin has reduced the amount of time it takes to complete a security review to just under four days.

"We're projecting our security posture outward to others," said Skyler Sampson, Senior Security Architect at Gremlin. "And the clearer and more consistent that information is, the less the prospect worries about our security."

Additional tips for using your security posture

Train salespeople on your security practices

Salespeople should have a high-level understanding of your security practices, so they can field questions and know where to go to get the right answers. This will also help to eliminate misinformation being spread about your security policies and procedures, which as mentioned previously, can cause trust to deteriorate between you and your customers.

Involve your security team in the sales process

Even when Salespeople are trained on your security practices, addressing complex security questions might not be in their wheelhouse. Working closely with your security team ensures that your prospects' questions are answered quickly and, most importantly, accurately.

This should also serve to accelerate the sales process as 65% of technology buyers say addressing security concerns caused delays in technology buying decisions, but only 29% of those buyers involved the security team in the process[10].

4

Centralize the management of vendor security

As more and more of the applications businesses use have moved to the cloud, managing and securing your environment has become more complex. And that's not just because you have less control over those applications, it's also because the number of vendors a typical business works with to run its day-to-day operations has increased significantly as well.

A typical technology company works with 133 vendors on average, but it's not uncommon for other industries like healthcare, manufacturing, and financial services businesses to work with nearly 100 vendors[11]. Keeping track of that many vendors and managing their assessment and reassessment can prove to be difficult if you're tracking everything in spreadsheets and corresponding over email.

Average number of third party vendors a technology company works with.

133

Minimize stress

Much of the stress that comes from managing vendor security assessments can be alleviated by implementing a centralized vendor database that gives you a view into all the vendors you're working with. A national insurance provider explains it this way, "You can't manage third-party risk, if you can't track your third parties[12]."

A good centralized vendor management database will let you see the status of each assessment, store all of your vendor certifications, and even integrate with your procurement systems to kick off new assessments or reassessments—all from one place. Incorporating automations in the vendor assessment process enables your team to be more focused on actually securing your environment. And isn't that the goal of every vendor security program?

Focus on what matters

Centralizing the security posture of all your vendors also provides your InfoSec and third-party risk teams with a better understanding of your overall risk and helps prioritize which vendors need additional follow up to give you peace of mind before engaging with them.

This was especially true for Marlette Funding[13], a market leader in online lending. Having a single source of truth for their vendor assessments gave them insights into which vendors were high risk and required a more thorough vetting process and which vendors had lower inherent risk and didn't require on-site follow-up.

Being able to distinguish between high and low risk vendors is important for Marlette Funding because there are significant costs associated with going on-site to evaluate vendors. Being able to eliminate unnecessary visits results in a large cost savings for the business, while helping them feel more confident about their overall security.

Conclusion

Over time, the need to effectively assess vendor security and third party risk is only going to increase.

Businesses that don't make efforts to modernize their approach to vendor security will play a constant game of catch up—whether they're responding to assessments or evaluating vendors. The good thing for you is modernizing your vendor security program isn't as hard as you think. Following the simple steps outlined in this ebook—using standardized assessments, being transparent, being proactive, and centralizing vendor security—will help get your program headed in the right direction.

[1, 6, 7] McKinsey & Company: Securing Software as a Service
[2, 3, 4] IBM Security: Cost of a Data Breach Report 2019
[5, 11, 12] Third party security risk management playbook
[8, 10] Gartner Brief: Proactively Address Security Concerns to Avoid Deal Delays
[9] Whistic Customer Case Study: Gremlin
[13] Whistic Customer Case Study: Marlette Funding

Following the four simple steps outlined in this ebook will help you get your program headed in the right direction.

1. **Rely on standardized assessments when you can**
   Standard questionnaires means responses will likely be faster, resulting in shorter buying and selling cycles.

2. **Be transparent**
   Be upfront and straightforward about the security practices you have in place to protect customer data.

3. **Take a proactive approach to vendor security assessments**
   Close deals faster and set yourself apart from the competition.

4. **Centralize the management of vendor security assessments**
   Keep track of your vendors and manage their assessments and reassessments.

How Whistic can help

For many businesses, security assessments are a double edged sword. They have to both evaluate vendors and respond to vendor assessments. With so many assessments coming in and out, it can be hard to keep a handle on everything.

To streamline the process for both the buying and selling side of the business, you should consider implementing a solution that can handle both sides of the assessment.

That's where Whistic comes in. Whistic is changing the way companies evaluate their vendors and build trust with customers.

- If you're a **buyer**, the Whistic Trust Catalog enables you to perform zero-touch assessments of your vendors in minutes—not weeks.
- If you're a **seller**, you can reuse the work you've done completing security assessments and share that information over and over again.

Visit whistic.com to learn more or to request a personalized demo.