whistic

HOW TO BUILD A VENDOR SECURITY PROCESS THAT HELPS SALES CLOSE DEALS FASTER

Tips for navigating vendor assessment requests that don't slow down the sales process

Introduction

In the aftermath of the COVID-19 pandemic, businesses were forced to accelerate their digital adoption strategy to help support a remote work environment for their employees and online interactions for their customers. This resulted in a spike in SaaS software sales that will only continue to grow in the coming years. Research by Google shows that cloud sales will triple by 2025 to $760B[1].

Bringing on that many new SaaS applications into your environment opens you up to potential data breaches unless you do your due diligence ahead of time and conduct thorough security assessments. The good news is that research by McKinsey has found that increased spending on data security will remain at pandemic levels[2], which means companies will continue to emphasize security into the future.

This massive shift to cloud-based applications has made navigating the vendor assessment ecosystem even more difficult than ever before. On the buyer's side, identifying and assessing new vendors is eating up countless hours of time for InfoSec and procurement teams. While on the flip side, InfoSec and sales teams are being inundated with questionnaires they need to respond to.

At the end of the day, both sides of the vendor security assessment process ultimately want the same thing—a secure environment free of breaches. Because they're coming at it from different angles, the process is often adversarial, but it doesn't have to be that way.

Over the course of this ebook we'll help you get your bearings in this increasingly complex ecosystem. We'll help you identify all of the different players, how they interact and work together during the vendor security process, and how vendor sales and InfoSec teams can navigate this new landscape seamlessly to close deals faster.

[1] https://www.saastr.com/google-says-will-triple-again-in-next-5-years/

[2] How COVID-19 has pushed companies over the technology tipping point—and transformed business forever - McKinsey, October 5, 2020

PART 1:

The Players

The number one priority of any vendor security program is to identify potential risks and remediate them in the hopes of preventing data breaches caused by vendors. Unfortunately, despite having a clear goal, there's no consensus on how to achieve it. Each business is different and as such has different security requirements. Fortunately, the ecosystem in which everybody operates is fairly similar across most businesses.

To help you get better acquainted with all the key players, we've provided a brief overview of each along with some context about how they fit into the ecosystem.

Enterprises (i.e. the buyer)

First up is the enterprise, or the buyer. There are a number of teams on the buying side that are impacted by the vendor security assessment process, including InfoSec, procurement, and the business sponsor.

Many of these teams responsible for identifying potential vendors, assigning inherent risk, assessing the vendor, and offering up a remediation plan are small. So when they were inundated with a massive influx of new vendors in the wake of COVID-19, they had a hard time keeping up.

The main goal of the enterprise buyer is to provide the business access to the solutions and services they need to succeed, while also keeping risk at manageable levels.

Vendors (i.e. the seller)

Next is the vendor being assessed. This group consists of the InfoSec team responsible for responding to questionnaire requests from the buyer as well as the sales team that is looking to close deals as quickly as possible, but whose deals might be slowed down by an inefficient questionnaire response process. Both sales and InfoSec teams are dealing with a lot of pressure around the vendor security assessment process.

For the sales teams, their livelihood depends on meeting quota and every deal matters, so if one deal pushes out to the next quarter because it took too long to respond to a questionnaire or if a security review kills a deal altogether, it could be the difference of making quota or being placed on a performance improvement plan.

InfoSec teams are often subject to the whims of the enterprises that they are selling to, many of which could be using custom questionnaires that can take longer to respond to because they are unknown quantities as opposed to standard questionnaires. And because these teams are small, it can often be difficult to keep up with all of the questionnaire requests that come across their desks each day.

Vendor assessment providers

Vendor assessment providers help both buyers and sellers streamline and automate many of the processes involved in responding to security questionnaires and assessing vendors. Buyers use these systems to manage the assessment process to ensure the third parties they bring into their environment have the proper security controls in place to protect customer data. Sellers use these solutions to build and share security profiles that contain completed questionnaires and other relevant information their customers might need.

Data Exchanges

Data exchanges, like Whistic, CyberGRX, or TruSight offer solutions to enable the re-use of data, questionnaires, vendor responses, documentation, and assessment validation. These exchanges gather information from primary and secondary sources and make it easier for InfoSec teams to make decisions about the potential risks a vendor might pose to their environment[3].

While there is a lot of good information contained in data exchanges, they may not provide all of the information needed to make an informed decision, so before deciding on how to incorporate data exchanges into your vendor security strategy be sure to do your due diligence[4]. For example, some exchanges are buyer driven and some are driven by sellers, meaning the vendor has more control over what is shared and can provide a more accurate picture of their security posture than if it only contained data aggregated from third party sources.

Industry Associations

Industry associations are content providers like Shared Assessments, Vendor Security Alliance, Cloud Security Alliance, and the Center for Internet Security who develop standardized frameworks that enterprises can utilize to assess their vendors.

While you might find that one standardized questionnaire will be enough to meet your security needs, they typically aren't one size fits all, so we recommend utilizing a combination of two or more questionnaires to ensure you have enough coverage.

Service providers and consultants

This includes professional service providers like EY, PwC, Deloitte, KPMG, as well as boutique consulting firms that help businesses build third-party vendor risk management programs, improve information security systems, or even respond to security questionnaires on your behalf. Consultants can be as involved as you want them to be. For example, if you lack the necessary experience or if your team is understaffed, a consultant can help you put the right frameworks in place and provide support for both responding to questionnaires or assessing vendors[5].

Security Rating Services

Security rating services like Bitsight, RiskRecon, and SecurityScorecard provide risk and security intelligence to enterprises assessing the security posture of potential vendors. But these services don't just help you make that initial decision, they help you monitor risk continuously throughout the entire vendor relationship.

[3] Navigating the Vendor Risk Management Solution Market, Gartner 2019

[4] Navigating the Vendor Risk Management Solution Market, Gartner 2019

[5] Navigating the Vendor Risk Management Solution Market, Gartner 2019

PART 2:

How to navigate the vendor assessment process so sales can close deals faster

The uptick in SaaS adoption is having a significant impact on cloud vendors. Virtually every sale they make requires them to respond to a security questionnaire. Sometimes it seems like there aren't enough hours in the day to respond to all of the requests, but if you make a few tweaks to your process highlighted in this section, you will save a significant amount of time for your InfoSec team while helping your sales team close deals faster.

Have clearly defined owners with clearly defined roles

Because security is involved in virtually every business-to-business transaction, it's important that you have all your ducks in a row. Having multiple functional groups, including sales and InfoSec responding to questionnaires might seem like the right idea, but having too many cooks in the kitchen can ultimately slow down the process.

Gartner suggests that determining clear roles and responsibilities should be the first step you take when building out your questionnaire response strategy—even more important than the technology you select to support your efforts[6].

The key is to collaborate and share information across the organization and make sure everyone knows what their responsibility is. Empowering sales to respond to portions of the questionnaires they know the answers to or to share their security profile early in the sales process is a good place to start, but if each team doesn't know what their role is, it could cause the sales process to grind to a halt.

Consolidate your security documentation in one place

Next, you'll want to collect all of your relevant security documentation—including questionnaires, certifications, audits, policies and other documentation (basically everything your customers need to assess your business)—and package it together so it's easier for your customers to review.

Fortunately, this is a growing trend and there are now solutions out there that can help you do this (including Whistic). Having all of your information in one place eases the burden on the InfoSec team and simplifies the assessment process for your customers.

Standout with Standards

There's a reason why standard questionnaires, like CAIQ, SIG, NIST 800-53, and VSA, are so popular. It's because they work. The questions and controls contained in them have been vetted by industry experts and are used by hundreds of thousands of businesses. That's why vendors should proactively conduct self-assessments using the most relevant questionnaires for the verticals they serve.

This will ensure that you are prepared to respond quickly when you receive a request from one of your customers—or even better, you can publish your security documentation publicly or share it with customers proactively before the request even comes in.

Provide on-demand access to security documentation

One place you can publish your security documentation is to data exchanges or marketplaces frequented by your customers. This makes it easy for customers and prospects to access your information in an environment that you control and helps them make informed decisions about whether or not your solution will fit well in their environment from a security standpoint.

Another good place to publish security documentation is on the security page of your website. Doing so puts the burden on your customer to request access and review your information, and allows your InfoSec team to focus on more strategic initiatives related to the security of your business.

Empower your sales team

In addition to publishing your security documentation to data exchanges and marketplaces and posting it on your website, you should also make it possible for your sales team to easily share that with customers. When this is done early in the sales process, it helps to build trust with customers and prospects and sets you apart from the competition.

Your business can have the best documentation in the world, but if sharing it causes a disruption in the sales process, your sales team will only share it if they absolutely have to.

Finding the right technology solution

In the past, InfoSec teams have had to deal with cobbled together systems where their security documentation was spread across multiple applications, which made it difficult to efficiently respond to security questionnaires or proactively share their profile. A good solution will help you consolidate all of the information and security documentation needed to build a detailed security profile and share it with prospects proactively before questionnaire requests even come in.

Additionally, the tool you choose should be built with collaboration. A collaborative tool breaks down silos that may have previously existed and enables your profile to be shared across the whole organization, ensuring that everyone is aware of the status of profiles after they're shared and whether or not your customer has viewed it.

Don't be afraid to ask for help

If you don't have experience responding to questionnaires or if your team is understaffed, there is a wide range of consultants available to help. Their services range from helping you define and set up your program all the way to groups that will manage the program end-to-end.

[6] How to Prepare a Third-Party Risk Management Framework, Gartner, June 2020

PART 3:

How sharing a security profile benefits your buyer

While building and maintaining a security profile makes navigating the vendor security assessment ecosystem simpler for the sales side of the equation, there are also many benefits that can be attributed to the buyer as well. Below we highlight some of the benefits that have the most impact.

Responses to security questionnaire requests are faster

According to the 2021 State of Vendor Security report, responses to security questionnaires can take nearly a week on average, and if clarification is needed that could add another four days per request[7]. Much of that time can be eliminated when sales teams build out and share a security profile.

Proactively sharing a security profile with your customers speeds up the buying process. Instead of sending out a questionnaire request, waiting for your response, and engaging in a lengthy back and forth, your customers have access to all the information they need to make a decision. And if they do need to follow up or request some clarification, it typically will be narrowly focused, so responses will be faster.

Help them achieve peace of mind

The threat of a cyber attack is more real than ever. Just this year the Solarwinds and Microsoft Exchange breaches impacted tens of thousands of businesses, and it seems like almost every day a new ransomware attack is reported in the news. The common thread most of these attacks have is that bad actors gained access through a third party vulnerability.

That's why your customers are so vigilant about third party security assessments. By delivering them a robust security profile that answers all of their questions and includes third party validation, you're providing them the peace of mind they need to choose you as a vendor.

Standard delivery of security documentation

In the past, your customers had to deal with cobbled together systems where their vendors' security documentation was spread out across multiple applications, spreadsheets, and email inboxes, which made it difficult for them to efficiently conduct a security review. By delivering them a nicely packaged security profile that contains all the information they need to make a decision about your business's security capabilities, you're not only making their job easier, but helping your solution stand out.

Publishing your security profile streamlines the assessment process

When you go beyond just sharing your profile on a business-to-business basis and make it available to anyone on the security and compliance page on your website or via a vendor security network, you're making the assessment process even easier for your customers. They can search you out, review your security documentation, and make a decision without any extra work on your part. Giving prospects the ability to do this means they can work on their timeline and your salespeople can focus on driving revenue to your business and not managing questionnaire responses.

[7] 2021 Whistic State of Vendor Security

PART 4:

Conclusion

The post-pandemic world we're approaching is vastly different from the one we lived in just over a year ago. Businesses had to adapt quickly to a more remote customer base and workforce, and as a result, adoption of SaaS solutions skyrocketed. This put a lot of pressure on InfoSec and SaaS sales teams responsible for responding to questionnaire requests.

Navigating this new landscape is not going to be easy, but if you have a plan in place with clearly defined roles, rely more on standard questionnaires, find ways to stay connected with your customers, and adopt the right technology to streamline and automate the process, you'll be heading in the right direction.

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 the network for assessing, publishing, and sharing vendor security information. With Whistic you can:

- Automate key activities in the vendor assessment process.
- Communicate the information your customers need, when they need it.
- Empower customer-facing teams to proactively share your security documentation.

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

whistic

www.whistic.com