



The 2022 State of Vendor Security

How cybersecurity and InfoSec trends impact
SaaS vendors and customers

Introduction

If 2021 taught us anything, it's that hackers and other bad actors are still targeting third parties as a means of entry into your environment to access and steal your valuable customer data. From SolarWinds to Microsoft Exchange and more recently the Log4j vulnerability, some of the biggest data breaches in history happened last year. While there's no way to completely eliminate data breaches from happening, we've found that when companies and their vendors are transparent and open about security posture and how each new application added to the environment impacts risk, the impact of breaches can be minimized.

Since our inception, Whistic has worked tirelessly to evangelize the importance of a thoughtful vendor assessment process for both buyers and sellers. We have a vested interest in understanding how current assessment practices are impacting businesses and what can be done to improve those practices in the future. That's why Whistic is committed to conducting regular research to ensure we maintain our position on the bleeding edge of vendor security.

In this report, the third in an ongoing series, we'll highlight the current state of vendor security, identify industry trends, and provide

recommendations for how companies can improve their processes for conducting and responding to assessments.

We partnered with a leading market research provider to conduct this research, utilizing their audience panels to survey more than 600 individuals working in InfoSec, cybersecurity, and SaaS sales. Two surveys were administered in late December 2021—one for InfoSec/cybersecurity and the other for SaaS sales professionals. The report is divided into two sections highlighting responses from each of the surveys.



InfoSec and Cybersecurity

Key Findings

The survey included responses from 315 individuals working in the cybersecurity and InfoSec industry. The respondents worked primarily for mid-sized enterprises, with an average company size of 1,332 employees. Despite working for larger companies, the respondents worked on relatively small teams with 5.8 members on average. Respondents ranged from manager to executive level and had 5.6 years experience in vendor security on average, with 13% having more than 10 years of experience.

Demographics



1,332 employees
average size of company



5.8
average size of team



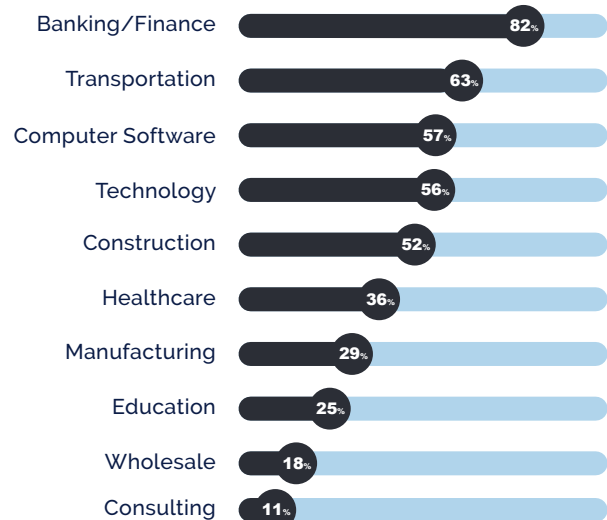
5.6 years
average experience

No company is immune to a data breach

Nearly half of survey respondents indicated they had experienced a data breach in the last

three years. When you dig in a little deeper at an industry level, there are some outliers. The rate of companies that have experienced a data breach the past year is slightly higher in technology (56%), computer software (57%), construction (52%), transportation (63%), and significantly higher in banking/finance (82%). There were also some outliers in other industries that had a lower percentage of respondents experiencing a data breach in the last three years, including manufacturing (29%), healthcare (36%), wholesale (18%), consulting (11%), and education (25%).

Rate of companies that have experienced a data breach



Of those who have experienced a data breach, 81% said the breach came as a result of a vulnerability in one of their third-party vendors. That number was quite a bit higher in banking and finance with 93% citing a third party as the cause for their breach, while 100% of those in retail said their breach was caused by one of their vendors. When it comes to cleaning up after the breach, respondents indicated it took 49 days on average to remediate and clean up.

Appetite exists for on-demand vendor assessments

Ninety-four percent of respondents indicated they would be willing to begin a vendor assessment by leveraging an already completed, on-demand questionnaire. This is up significantly from last year's report when just 82% of respondents indicated a willingness to conduct on-demand assessments.

On the vendor side, 80% of respondents said they would be willing to make security documentation available publicly to customers and prospects so long as they had the ability to control who sees it and for how long. Below is a breakdown of places they would be willing to publish that documentation.

- **Security page on their website (70%)**
- **Review portals like G2 (55%)**
- **Exchanges like CSA STAR Registry or the Whistic Trust Catalog (43%)**

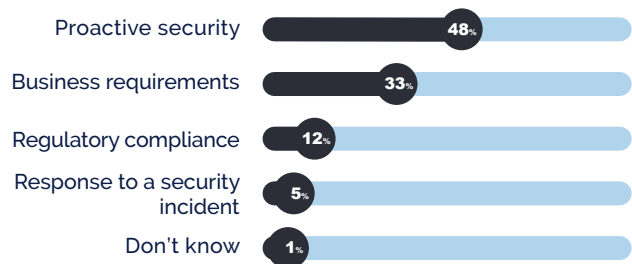
Respondents also said having access to on-demand questionnaires would save them 12.4 hours per month assessing vendors.

Proactive vendor security remains a key motivator

Proactive vendor security and protecting sensitive data remain the number one

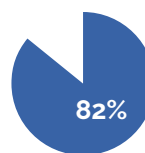
motivator for companies to start assessing vendor security. This is followed by customer or industry requirements, regulations like HIPAA, GDPR, FFIEC, and finally in response to a security incident. This is consistent with results from previous surveys.

Why companies start assessing vendor security



Use of third party validation increasing

The number of respondents who indicated their companies use risk ratings or scoring providers as part of the vendor security process increased significantly year over year, growing from 59% in 2021 to 72% in 2022. This shows an increased value in third-party validation of a vendor's questionnaire response when evaluating potential vendors.



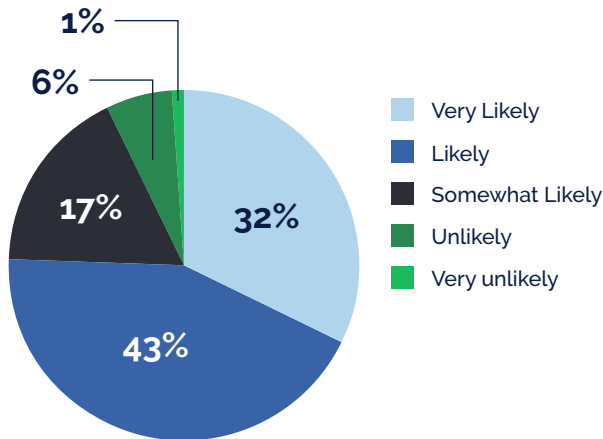
When asked how important on a scale of 1-10 continuous monitoring and live risk ratings were to the vendor assessment process, 82% rated it an 8 or higher.

More than SOC 2 and ISO 27001 needed

Despite the obvious need for third party validation of vendor security posture, vendors can't just provide their customers with a SOC 2 or ISO 27001 and call it a day. Even though those reports are very thorough, only seven percent of respondents said they would require no additional security documentation.

These reports are a good starting point, but it is important to include responses to industry-standard frameworks and other information relevant to your security posture.

If the vendor provides a SOC 2 or ISO 27001, how likely would you be to ask for additional security documentation?



Number of vendors assessed on the rise

The survey found that the number of vendors assessed annually, on average, increased by 20%, from 141 to 172. While the number of vendors companies manage in their environments decreased slightly from 160 to 157. This could be due to a number of factors, from consolidation of applications to the difference in audience from year over year.

The vendor assessment process is time consuming for buyers and sellers

Vendors surveyed are responding to 23 vendor assessment requests each month on average, which is an increase of approximately 10% from the previous year. With each response taking around 3.5 hours—that's 80.5 hours per month.

But that's just the raw hours it takes to respond to a questionnaire request. In terms of the sales

cycle, it can add up to a week before the deal is closed, and if there's a clarification request from the customer, it can take even longer. Each clarification request adds 4.1 days to the sales cycle on average. What these numbers don't show is how responding to questionnaire requests disrupts the day-to-day activities of InfoSec and cybersecurity teams. Instead of creating a secure environment, they are tasked with administrative duties.

When it comes to assessing vendors, respondents are spending 23 hours per week, and it typically takes 4.8 days to receive completed assessments back from vendors. It's interesting to note that the top two most time-consuming aspects of the vendor assessment process are adding little value to improving security. It's focused on what information do I need and who do I need to get it from—tasks that can be easily automated with the right technology.

Top time-consuming aspects of the vendor assessment process:

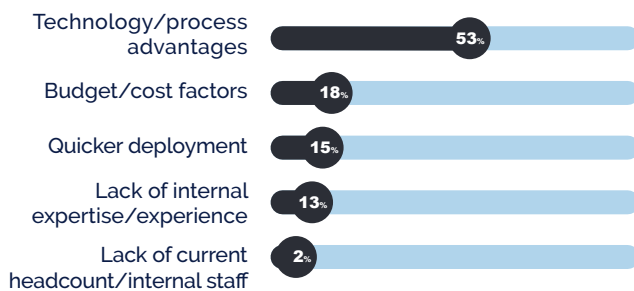
- **Determining vendor risk levels and what information to request from the vendor (33%)**
- **Tracking down vendor contact information and other relevant info from internal stakeholders (26%)**
- **Reviewing vendor responses, identifying gaps/risks, and writing up a final summary of the assessment (21%)**
- **Discovering which vendors need to be assessed (15%)**
- **Communicating the results of the vendor assessment internally to the vendor and working through any remediation or follow-up tasks (5%)**

This differs from the previous year, which listed the following as the most time-consuming aspects of assessing vendors:

- Reviewing vendor responses, identifying gaps/risks, and writing up the final assessment (28%)
- Determining vendor risk levels and what information to request from the vendor (23%)
- Tracking vendor contact information and other relevant info from internal stakeholders (22%)
- Discovering which vendors need to be assessed (18%)
- Communicating the results of the vendor assessment internally to the vendor and working through any remediation or follow-up tasks (8%)

Teams outsource at least some of the process to increase efficiency

Sixty percent of survey respondents are outsourcing at least some of the vendor assessment process, with 15% outsourcing the entire process and 45% of respondents using a mix of internal and external resources. The primary reasons for outsourcing are as follows:



Still no industry standard for assessing vendor security

The survey found that 30% of companies surveyed are using custom, non-standard questionnaires, which is up slightly from the previous year, with 52% using a combination of industry standard and custom questionnaires and 15% using only industry standard

questionnaires and frameworks to assess vendors.

However, 51% of those surveyed also said they were considering implementing or adopting industry standard questionnaires in the future and 38% indicated it was a possibility. This is up from the previous year where 48% were considering implementing standard questionnaires and 29% said it was a possibility.

Top Industry Standard Questionnaires and Frameworks







SaaS Sales Survey

Key Findings

For this portion of the report, we surveyed 303 sales representatives working in SaaS. Respondents worked primarily in technology and computer software, which was to be expected, but a small percentage worked for SaaS companies in specific industries like healthcare, finance, retail, etc. On average, they had 6.5 years experience working in SaaS sales, have titles ranging from SDR to CRO, and worked for medium to large enterprises with an average company size of 1,620 employees.

Demographics

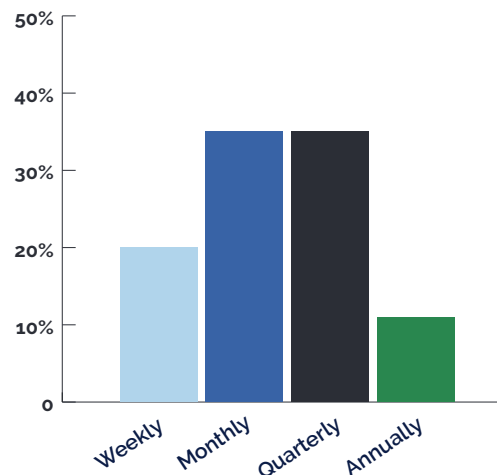
	1,620 employees average size of company
	6.5 years average experience
	Technology and Computer Software Industry
	Director (44%), Account Executive (16%), VP of Sales (8%), CRO (6%) Most common titles

Proactive sharing of security information on the rise

Sixty-four percent of salespeople surveyed indicated they proactively share security documentation with customers and prospects, which is up from 58% the previous year.

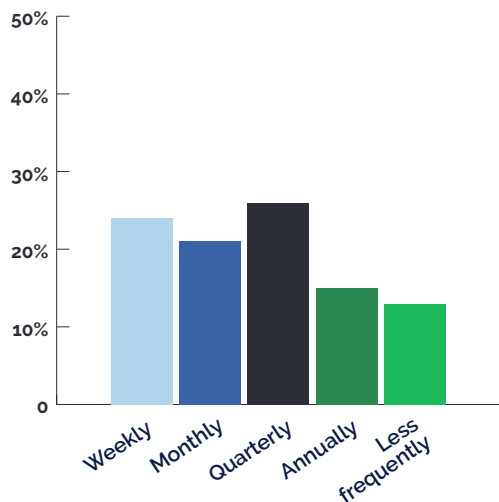
Sharing security information early in the sales process helps ensure deals close faster, resulting in fewer deals pushing to the next quarter or being lost altogether because sales teams can't respond quickly enough or show their company can meet their customers' security needs.

Frequency a deal pushes because you couldn't respond to a security review in time



Forty-five percent of respondents said they had a deal push because they couldn't respond to a security review in time. This is up eight percent from the previous year where 37% of respondents made that claim.

Frequency a deal is lost because you couldn't respond to a security review in time or meet the customer's security expectations

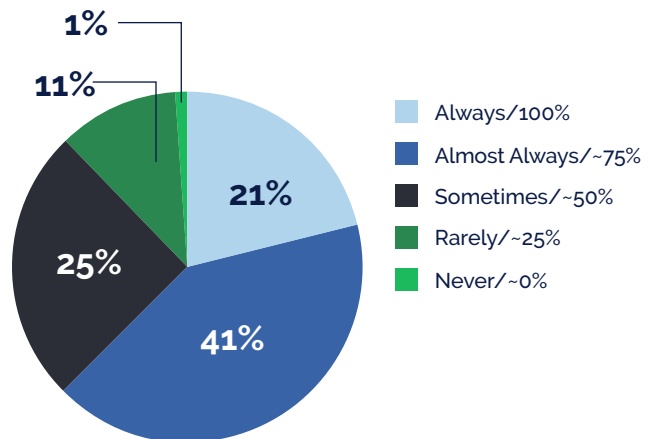


Another 34% indicated they lost a deal because they couldn't respond to a security review in time or meet the customer's security expectations. This number remained consistent year-over-year.

Sales reps responding to security reviews instead of driving revenue

There are only so many hours in a day and only so many selling days in a quarter, and any time your sales reps spend doing administrative work like responding to security reviews takes them away from what they do best—closing deals. Unfortunately, many salespeople are still having to spend a significant amount of time tracking down answers to questionnaires.

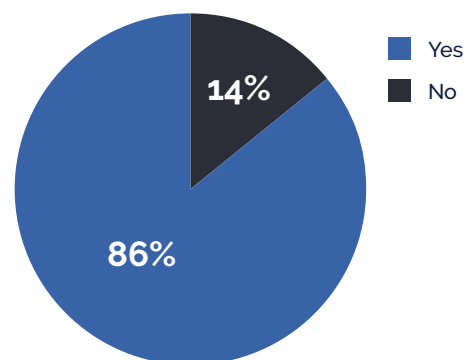
How often sales reps are involved in responding to a security review



They are spending 7.4 hours, or the equivalent of nearly one working day per month responding to security reviews, with 22% of respondents spending more than 10 hours per month. This is up slightly from the previous survey, which found that sales reps were spending 6.8 hours per month on average answering security questionnaires.

The survey also found that revenue increases when efforts are made to streamline the vendor assessment process.

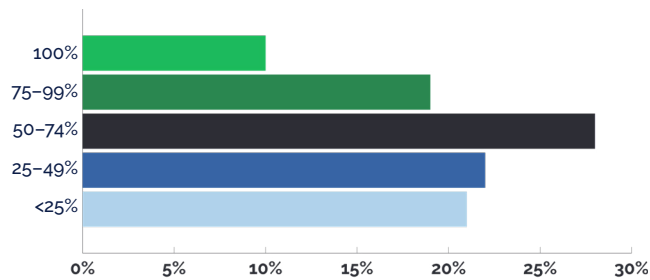
Would streamlining customer security reviews help me generate more revenue for my company?



Responding to questionnaires lengthens the sales cycle

Seventy-nine percent of respondents said their customers require them to respond to a security review/assessment before they close a deal and that responding to a security review adds a week to the sales cycle. That number is even higher if clarification is required on the returned questionnaire, which as we noted in the previous section, adds another four days to the sales cycle.

Percent of deals that require clarification



Recommendations

Based on the results of the survey, there are a few key areas we believe if you make slight adjustments to your existing strategy, will pay huge dividends in improving the vendor assessment process, resulting in faster sales cycles and a more efficient and secure security ecosystem.

Build a thorough security profile and share it proactively

While the survey found that custom questionnaire use is on the rise, we still recommend basing your security profile on standard questionnaires commonly used by your customers. Most of your customers are willing to begin the assessment process with an already completed questionnaire, so all you would need to do in the future is respond to clarifying questions, which will take significantly less time than responding to an entire custom questionnaire. When building your Profile, we suggest including the following elements:

Complete standard questionnaires. While it might seem like a lot of work to complete three to five standard questionnaires up front to build your security profile, it will save you a lot of time in the long run and ensure your security posture has been properly vetted for

your customers and prospects. And if you're worried about customers accepting standard questionnaires, you shouldn't be as most custom questionnaires use questions from standard frameworks as a baseline.

Put an NDA in place. To ensure your security posture remains protected, we recommend attaching an NDA to your Profile before it can be accessed.

Upload audits and certifications. We'll talk about this a little later in the recommendations section, but third-party validation of vendor attestation is becoming increasingly important. As such, any Profile worth its salt will include things like a SOC 2 Type 2 report, ISO 27001, FEDRAMP, or any of the certifications and audits you may have completed.

Once your Profile is completed, package it up nicely and give access to your salespeople, so they can start sharing it proactively at the outset of any sales cycle. Being transparent (as you'll see below) helps build trust with your customers because it shows you have nothing to hide.

Look for ways to be more transparent

As our research shows, most transactions require some form of security assessment before they can be completed. Since this is the case, we recommend vendors get out in front of the process and publish their security profile publicly. Being transparent with customers helps build trust at the outset of the relationship and increases the likelihood of them purchasing from you. To help you get started, we recommend publishing in the following places:

The security page of your website. The easiest and most obvious place to publish your security documentation is on the security page of your website. Depending on how much control you want to have over your documentation, there are a number of solutions (including Whistic) that can host your documentation and manage the requests. These solutions give you the opportunity to decide who has access to your information, for how long, while also helping ensure they have the most up-to-date version of your documentation.

Security directories and exchanges. Next, you should identify directories and exchanges that your customers frequent to conduct on-demand assessments of vendor security posture like CSA's STAR Registry or Whistic's Trust Catalog and publish your Profile to them. Making your security posture available on-demand speeds up the vendor assessment process, provides a better experience for your customers, and saves the time your InfoSec team used to spend responding to one-off questionnaire requests.

Software review sites. Finally, many software review sites, like G2, are incorporating security documentation to their portals to help users

make the most informed decisions about software purchases. One of the biggest reasons is because security is often cited as the most important factor in determining which vendor is chosen.

Incorporate more third-party validation in assessments

The increase in risk ratings usage indicates that companies see an increased value in third-party validation of security information, but risk ratings are just scratching the surface of third-party validation available. Below are some other examples we recently highlighted in an ebook about 2022 trends in vendor security:

Internal validation by vendor. First, you can ask the vendor to conduct control compliance self-validation using a tool like Drata or Whistic and provide a time-stamped report that shows control compliance data as evidence.

Independent audit or certification. One of the best and most common methods for validating a vendor's security compliance is via a third-party audit like a SOC 2 Type II or an ISO 27001 Certification provided by the vendor.

Third-party risk assessment. If you feel the need to go above and beyond, when validating vendor assessments, you can hire a third-party assessor to conduct an assessment of your vendors. This validation method is more costly than the others, but it is very effective at helping identify risk associated with your vendors.

Internal continuous validation. Finally, you can utilize a continuous compliance tool like Drata to automatically and continuously validate control compliance of your vendors.

Keep your sales team selling

It's no secret that responding to questionnaires can be a time-consuming process and can take valuable selling time away from your reps. But when you incorporate strategies like the ones outlined above into your process and enable your sales team to share your security posture proactively, they can focus on what they do best—driving revenue.

Are you putting security first?

Join top tech firms committed to put security first by pledging to proactively share your security documentation with customers.

[Join Security First Initiative](#)

Founding members of the Security First Initiative



▲ ATlassian

okta



●● asana

TripActions



whistic



How Whistic can help

For many businesses, vendor security is 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
- Build trust with customers and vendors through transparency

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





www.whistic.com