



20  
23

WHISTIC REPORT

---

State of  
Vendor  
Security

Across every industry, 2022 was another record year for third-party vendor security incidents. Companies running the gamut from DoorDash (technology), to KeyBank (financial services), to hundreds of school district customers of Illuminate Education (education), and Highmark Health (healthcare) experienced a data breach that originated with a compromised third-party vendor. Data breaches like these can't be prevented with certainty, but the damage they do is real: it can take years to repair a business's reputation after a breach and the average cost of a data breach in the U.S. is now an astounding \$9.44M!<sup>1</sup>

As long as there are firewalls to be penetrated and data to be stolen, hackers will continue wreaking havoc upon InfoSec teams by exploiting weak links in a company's third-party vendor ecosystem. Today more than ever, organizations must pursue opportunities to reduce the likelihood of an attack and minimize the impact if one does occur.

One approach has been proven to reduce both the likelihood and impact of third-party vendor security incidents: **transparency and collaboration between businesses and vendors.**

When vendors and their customers collaborate and are transparent during the vendor security review process, they can build a stronger defense against attackers by focusing time and effort on potential areas of exposure instead of wasting that precious time on administrative tasks associated with the vendor assessment. However, not all businesses understand the importance of transparency and its undeniable impact on trust and security.



\$9.44m

Average cost of a data breach  
in the U.S.

---

---

<sup>1</sup><https://www.ibm.com/reports/data-breach>

# Introducing Whistic's 2023 State of Vendor Security Survey

In this report, we will reveal the results from Whistic's third annual **State of Vendor Security Report**, as well as identify trends in vendor security and provide recommendations for what businesses can do to improve both transparency, vendor security, and vendor risk program maturity.

Before we get started, let's dig into the methodology used to conduct the survey. Whistic worked with a leading automated research firm to survey more than 500 cybersecurity and Information Security professionals at the manager level or above.

- 524 cybersecurity and InfoSec professionals surveyed.
- 36% of companies surveyed were in the technology industry, with 20 other industries represented.
- Respondents were predominantly manager or director level, with 22% being C-level.
- 60% of respondents have both the responsibility for assessing vendors and responding to security questionnaires from customers.
- The majority of companies had between 500 and 5,000 employees.



500–5,000

Employee size of most companies surveyed



36%

Companies surveyed that were in the technology industry

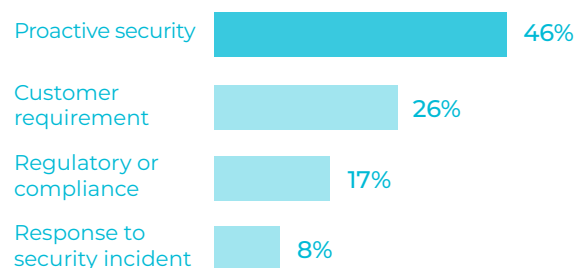


60%

Respondents who have both the responsibility for assessing vendors and responding to security questionnaires from customers

# Why assess vendors? The sobering impact of data breaches

Before we jump into the bulk of the survey findings, let's briefly explore a fundamental question: Why do companies assess vendors? While there are a number of reasons companies establish a vendor assessment process, securing sensitive data takes the top spot according to the 2023 survey data. Forty-six percent of companies surveyed indicated that "proactive security" is the primary reason for their vendor security program. Other reasons included: business requirements from customers (26%); regulatory and compliance requirements (17%); and response to a security incident (8%).



## Reasons companies establish a vendor assessment process

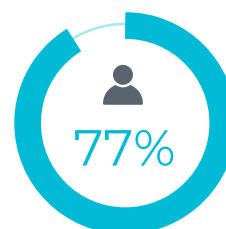
As evidence of the importance of proactively establishing a program to assess vendor security, 54% of respondents indicated that they had experienced a data breach in the past three years—an increase of seven percentage points from our 2022 survey, where the same question resulted in 47%. And here's the can't-miss

bottom line: a stunning 77% of respondents who had experienced a data breach said the breach was the result of a compromised vendor.

As we now prepare to explore the results of this comprehensive survey, it's important to keep in mind that according to this study, the driving force behind any vendor assessment program ultimately stems from a desire to meet one or more of these three fundamental outcomes:

1. Securing sensitive data.
2. Meeting business and customer requirements.
3. Meeting regulatory compliance or audit requirements.

The survey focused on two primary areas: 1) the vendor assessment process, and 2) the security questionnaire response process. We'll begin by examining the vendor assessment process.



Respondents who experienced a data breach who said the breach was the result of a compromised vendor



SECTION ONE

---

# Vendor Assessments

# 1 Significant time spent assessing vendors

We found that respondents spend considerable time assessing vendors to ensure they aren't caught up in the next third-party vendor data breach. Nearly 40% of companies surveyed have over 100 vendors, with 30% having between 50 and 100 vendors. Companies indicated that the number of vendors they assess each year mirrors the total vendor population, with nearly 40% of companies assessing over 100 vendors per year. The typical team assigned this responsibility is four to six people, with 43% of teams having 7 or more people. The vast majority of respondents (over 75%) have multiple teams or departments with their company that get involved in conducting a vendor assessment (i.e., Information Security, IT, Compliance, Legal, etc.).

**Over 50% of teams are currently spending over 20 hours per week assessing vendors, with over a third of companies spending greater than 30 hours per week**—which is greater than the 23 hour average spent per week in 2022. The majority of companies indicated that it takes longer than one business week to receive a vendor's initial response to an assessment request, with companies indicating that 40% of the time the response or initial documentation is missing information. If clarification is needed, add another 4.4 days on average to the process. And that clarification is needed quite often (85% of the time): 12% indicated clarification is always needed; 44% said "almost always," and 29% said "sometimes."

When asked about the actual work completed by their team (and not the vendor) in the assessment process, nearly two-thirds of respondents (64%) indicated that the preparatory work that enables a professional to perform a vendor assessment was the most time consuming aspect of the assessment (i.e. discovering which vendors need to be assessed, what type of information to request, tracking down vendor information, getting relevant details from business stakeholders, etc.)

While 37% of those surveyed are doing all the vendor assessment work in-house, another 45% sought some help from outsourced vendor assessment practitioners. The remaining 18% outsourced the entire process. This is fairly consistent with 2022 survey results, where the numbers were 40%, 45%, and 15%, respectively. For teams that outsource vendor assessment work, the primary reason for doing so was technology or process advantages.



Number of vendors indicated by companies surveyed, by percentage

## 2 Use of assessment software and standardized frameworks

Sixty-seven percent of respondents indicated they were currently assessing vendors using a tool purpose-built for that task, while 33% were still using spreadsheets and other manual assessment processes. This indicates a strong upward trend towards more adoption of software to automate and streamline the vendor assessment process when compared to survey results from just two years ago when only 57% of companies indicated that they had adopted vendor assessment software.



Increase in respondents who indicated they were using a vendor assessment software

Ninety-eight percent of companies use a questionnaire as a part of their vendor assessment process with a majority of respondents (62%) using a combination of standardized and custom framework questionnaires when assessing vendors. 20% use custom questionnaires exclusively, while 16% use only standard questionnaires. Of those that aren't currently using standardized questionnaires, 54% said they are considering using them in the future, indicating a strong trend towards more standardization in the future.

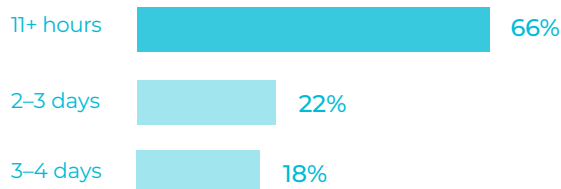
Businesses that want to see quicker turnarounds would be wise to rely more heavily on standard questionnaires and frameworks. They have been built and vetted by industry experts and leaders to ensure that they cover the most important controls. They are also more easily maintained as new versions are regularly published by industry bodies. As a best practice, Whistic suggests identifying the standardized questionnaires most relevant to your industry and aligning with those frameworks when assessing your vendors, such as HIPAA, GDPR, ISO 27001, and CAIQ.



Companies using a questionnaire as a part of their vendor assessment process

# 3 Significant opportunity for time and cost savings

By aligning with standards, organizations will also more readily benefit from vendors who have already completed a version of the framework, reducing the turnaround time required to complete an assessment. A key finding supporting this: with more than two-thirds of companies indicating that the most time-consuming portion of the assessment is in tracking down vendor information in order to prepare for an assessment, nearly two-thirds (66%) of respondents estimated they could save more than 11 hours per month assessing vendors if security documentation was made available on-demand. Twenty-two percent of respondents indicated that they would save even more time, with 2–3 business days worth of potential time savings (16–20 hours). Significantly, 18% indicated that they could save 3–4 days per month (21–30 hours of work) by leveraging pre-completed, standardized questionnaires like the ones published by thousands of companies in the Whistic Trust Catalog!



Estimated times savings if security documentation was available on-demand, per month


This data is supported by Whistic's own platform data. Whistic data shows that the average time it takes to receive a completed questionnaire from a vendor is 12.7 days, while the time it takes to find a vendor's Profile in the Whistic Trust Catalog is less than two minutes. In other words, by conducting a Zero-Touch Assessment® utilizing a Profile published via the Whistic Vendor Security Network, you can reduce turnaround time by 99%!

12.7 days to  
<2 minutes



Questionnaire completion time reduction if using a Whistic Profile

99%

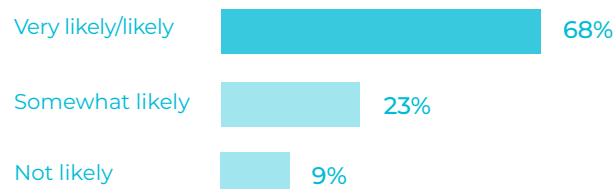


Percentage of reduced turnaround time when conducting a Zero-Touch Assessment™ utilizing a Whistic Profile

Some vendors may assume that because SOC 2 and ISO 27001 audits are conducted by an independent third party that they will satisfy customer requirements without the need for a security questionnaire. This assumption is not



supported by the data: 68% of respondents said it was “Very likely” or “Likely” that they would request additional documentation from vendors AFTER receiving a SOC 2 or ISO 27001 report. Another 23% said it would be somewhat likely. Only 9% said it would be unlikely they would request additional information in this scenario.



Respondents indicating additional documentation would be requested after a SOC 2 or ISO 27001 report

When coupled with the data indicating that nearly half of assessments require clarification due incomplete responses or documentation, and when factoring in the time it takes to receive a completed questionnaire along with vendor clarification, we found that it takes an average of 17 days to receive a complete vendor assessment response!

# 17 days

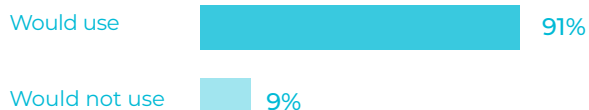


Average number of days saved using pre-published vendor information

This leads us to one of the most important best practice findings of the study: if vendors will proactively publish a comprehensive Profile containing pre-completed standardized framework questionnaires, audits and certifications, and other supporting documentation, they can eliminate a whopping

17 days out of the sales process on average! The data shows that more and more companies are willing to do this with 79% of respondents stating that they would be willing to make their security documentation available publicly to customers as long as they have the ability to control who sees it and for how long.

On the flip side, when teams performing assessments are willing to leverage pre-published vendor information, they are able to eliminate an average of 17 days from their assessment and purchasing process! The data supports that the vast majority of teams performing vendor assessments are looking for solutions that can provide this capability, as 91% of respondents said that they would be willing to begin each of their vendor assessments by leveraging pre-completed, on-demand standardized questionnaires.




Respondents who would be willing to begin their vendor assessments using a pre-completed standard questionnaire

# 4 Vast majority of businesses utilize risk ratings

The use of risk ratings as part of the vendor assessment process held relatively steady year over year, with 73% of respondents indicating that they were utilizing risk ratings (an increase of 1% from last year). Eleven percent responded they were considering incorporating risk ratings, while 16% responded they were neither using nor considering including risk ratings in the future.

Respondents were also asked to rate (on a scale of 1 to 10) how important continuous monitoring and live risk ratings are as part of the vendor assessment process. 67% of respondents rated it either a nine or ten (no surprise when considering the 73% using risk ratings already).

Why is continuous monitoring such an important part of a vendor risk management program? Questionnaires are only a point-in-time view of a vendor's security posture. And if there's one constant in vendor risk, it's that it is always changing. The "outside-in" view into the cyber risk of an organization that risk ratings provide also complements the "inside-out" view that vendor assessment questionnaires and documentation provide.



Whistic demonstrates the powerful intersection of these two capabilities by integrating ratings by RiskRecon, a MasterCard company, into the more than 50,000 Profiles found in the Whistic Trust Catalog.

# 5 Vendor Security continues to gain importance at the C-level

Fifty percent of respondents said C-level executives are very involved in the vendor security process and results at their companies, while 41% said execs are at least somewhat involved. The 91% of companies with C-level backing for their vendor security program indicates a strong upward trend towards more support at the executive level for this important priority.

In addition, 86% of companies stated that running a proper vendor security program is at least an "8 out of 10" (when asked to rank it on a scale from 1-10) in importance to their company (as indicated by the amount of resources, policies and procedures allocated to it), with the largest segment (36%) indicating that it couldn't be more important: they ranked it a "10 out of 10" in importance. Only 6% of companies indicated that it was a 5 or lower on the scale of importance, which demonstrates the continued focus on improving vendor security at companies across nearly every industry.



Companies that ranked a proper vendor security program as most important

# 6 Standing up a vendor security assessment program

When creating a vendor security assessment process, we recommend several best practices as you get started:

- 1. Automate vendor intake.** When you don't have the right tools in place for vendor intake, finding the information needed to initiate the assessment can exhaust time and resources. An effective vendor intake process gathers all the necessary information required to assign inherent risk and proceed with an assessment plan based upon risk designation.
- 2. Decide on an assessment methodology.** Assessment frequency and thoroughness should both be determined by inherent risk assigned at intake as well as the criticality of the product or service and taking into consideration the specific use-case. For example, if you have a high-risk cloud vendor that is critical to your operations, assess them annually AND validate all of the most important controls. On the contrary, a low-risk vendor will require a minimal assessment and may only require a one-time assessment.
- 3. Trigger assessment requests automatically.** The assessment request process should be as hands-off as possible. Assessment requests should be triggered once risk levels are assigned and reassessment requests should be automatically sent at the time determined in your assessment methodology.
- 4. Conduct Zero-Touch Assessments when possible.** The best and most effective method to conduct vendor assessments is searching out vendors that are transparent regarding their security posture and publish it publicly on places like the CSA STAR Registry and Whistic Trust Catalog. Vendors who proactively share security information help you build a relationship on a foundation of trust and enable you to focus on what matters most, as opposed to spending the majority of your time chasing down information. It doesn't hurt that you'll also potentially receive the completed questionnaire and documentation in minutes, not weeks.



SECTION TWO

---

# Security Questionnaire Response

# 1 Responding to vendor assessments

Responding to security questionnaires can be a painstakingly repetitive and time consuming process that slows down sales cycles and negatively impacts the likelihood of a new customer relationship closing. But how much time does the average vendor spend responding to questionnaires?

Fifty-four percent of vendor respondents in the survey reported that they answered more than 11 security questionnaires each month, with over 20% responding to over 26 per month and 9% responding to over 50 per month. With the majority of companies (54%) spending 1-4 hours per security questionnaire response, and 26% spending between 5-10 hours per response, this equates to the average company spending 7 business days (~50 hours) of team resources per month responding to security questionnaires!

With that as the backdrop, it is no wonder why so many companies are searching for ways to reduce the burden that these security questionnaires create. 79% of respondents said they would be willing to publish their security documentation publicly on their website or on directories like the CSA STAR Registry, Whistic Trust Catalog, or reviews sites where purchase decisions are being made. This strategy makes it easier for their prospects and customers to conduct assessments without needing to request that the company complete a security questionnaire, saving the dozens of hours per

month that the average company dedicates to this activity.

This trend towards more proactively and transparently publishing security information is right in line with the companion trend of more companies being willing to accept this type of information as a part of their assessment process. It also points to the real friction that the traditional questionnaire-based assessment process creates on both sides of the vendor assessment process.



Respondents who would be willing to publish their security documentation publicly on their website or directories




Percentage of companies spending more than 50 hours of team resources to respond to questionnaires

## 2 Equip and empower your sales team— and impact your bottom line

As if that data weren't painful enough, close to two-thirds of companies (64%) also indicated that a sales representative is "Almost Always" or "Always" involved in responding to at least a portion of the security questionnaire. Not only is this impacting company costs from a "time allocated" perspective, it is also impacting revenue as sales representatives are spending their time away from selling when responding to questionnaires. You hired your sales team to drive revenue, not deal with security reviews. This is time they could spend talking to prospects, demoing your product, or conducting other revenue-generating outreach efforts.

Building a Whistic Profile frees up your sales team to focus on what they do best—closing deals and generating revenue. Customers get all the security information they need immediately. That's because sales can point them to a link to your Whistic Profile or share it directly with them via our Salesforce or Slack integrations.



Whistic Profile allows your sales team to focus on what they do best—closing deals and generating revenue. Now, they can share security information with customers directly or via the Salesforce or Slack integrations.

---

# 3 The drive for improvement and progress in vendor assessments

More than half of respondents, while generally satisfied with their vendor assessment process, agree that it could be improved. However, 46% of respondents indicated that the vendor assessment process is better than it's historically been.

The 2023 State of Vendor Security Survey reveals that companies are increasingly adopting proactive security and assessment measures on both sides of the vendor/customer relationship. But the industry still lacks a generally acceptable standard of trust and transparency needed in order to truly transform the legacy processes that plague the professionals responsible for vendor assessments across the globe.

To address this seemingly monumental problem, Whistic helped found the [Security First Initiative](#) in early 2022 alongside some of the world's leading tech companies, including Okta, Airbnb, Zendesk, Atlassian, Snap, Notion, and Navan.

Members of the Security First Initiative have invited companies everywhere to:

- Build and maintain a security profile that contains relevant standard questionnaires, certifications, and audits.
- Share that information publicly and proactively with their customers using the Whistic Vendor Security Network.

- Create the expectation that every company they do business with adopts the same approach.

When businesses implement transparent vendor security practices and foster collaborative relationships with customers, they begin to create an environment where the vendor security ecosystem can be better protected against future vendor data breaches.



# Whistic is here to help


As demonstrated by the data in this survey, there are a lot of positive trends related to vendor security, but there are also a lot of areas where companies could use help. Whistic helps companies mitigate risk, reduce costs, and enable revenue by:

1. Automating the vendor risk management process. The vendor assessment lifecycle is a complex, multi-step process that begins prior to an official legal relationship and often extends for years in the future. Whistic automates many of the steps in that process from initial vendor intake to ongoing reassessment and enables companies to reduce risk by maturing their vendor risk management programs.

2. Facilitating Zero-Touch Assessments. Once a vendor's Whistic Profile is published to the Vendor Security Network, companies can easily search, find, and connect with vendors they need to assess. Once they find the business they're looking for, they can access security documentation immediately and begin the assessment process, eliminating weeks of inefficient back-and-forth. When coupled with the additional automation capabilities Whistic provides, this can significantly reduce costs, headcount and ensure a more effective use of resources.

3. Enabling sales teams to be transparent and proactive. With a Whistic Profile, vendors can compile all their security documentation, including certifications, audits, and industry-standard questionnaires and frameworks, into one central location. From there, vendors can enable their sales team to proactively share their Whistic Profile with customers early in the sales process and publish to their website or the Whistic Vendor Security Network. This shortens sales cycles, accelerates business, and transforms security teams from a cost-center into a revenue enabler.

Ready to learn more? Find out how Whistic can help your business improve its vendor assessment process by [requesting a demo today](#).



Whistic helps companies  
mitigate risk, reduce costs,  
and enable revenue.



[www.whistic.com](http://www.whistic.com)