whistic

2023 Vendor Security Trends to Watch

As we enter a new year, it's a good time to reflect on the events of the past year and how they impact our plans and strategies for the coming year. This past year, like the year before, was filled with high profile breaches. Whether it's Crypto.com or Microsoft earlier in the year or more recently Uber and Rockstar Games, companies of all sizes and types were susceptible to an attack

The good news for infosec and cybersecurity practitioners is that their jobs seem more secure than ever. The bad news is that job security comes as a result of hackers relentlessly trying to breach their companies to steal data or force them to pay hefty sums during a ransomware attack.

Because attacks are becoming more and more sophisticated and increasing in number, we've outlined a number of trends in this ebook we're following and suggest you follow as well to help companies stay a step ahead of the bad actors trying to take your company down.

Along with these trends, we'll be providing readers with best practices that can be easily incorporated into your vendor security strategy. The trends we're watching include:

1. **Transparency**
2. **Deepen integrations with procurement**
3. **Shift left**
4. **Zero-Touch**
5. **Real-time/live security documentation**
6. **Transparency via Automation**
7. **Environmental, Social, Governance**
8. **Fourth-Party**

Trend #1: Increased transparency between vendors and their customers

Transparency as a concept is nothing new, but as attacks become more targeted and more nuanced, it's going to take a collaborative effort between companies and their vendors to ensure breaches don't happen, and if they do happen, they're caught early and mitigated quickly to lessen the damage.

In the past there were movements toward zero trust when it came to third parties, but we feel complete transparency between vendors and customers is a better approach. At the end of the day, everyone has the same goals—to identify potential risks and prevent incidents from happening.

The biggest step forward vendors can make when it comes to transparency is the timing of when they share security documentation with customers and prospects. There was a time when vendors waited until the absolute last minute to respond to questionnaire requests. That's because the process of responding to questionnaires was less than ideal. The questionnaires came in excel spreadsheets and the answers were spread across the organization, so it could take hours or even days to complete.

Now, it's much easier to proactively build and share a security profile with your customers. Before you say your customers won't accept pre-completed standard questionnaires, let me stop you right there. Research by Whistic shows that 96% of companies said they would be more likely to purchase from a vendor that is transparent about its security posture[1] and 90% of companies indicated they would be willing to begin a vendor assessment by leveraging an already completed, on-demand questionnaire[2].

Incorporating transparency into your strategy

The first thing that vendors should do is compile all of their security documentation, including the standard questionnaires and frameworks that are most commonly used in your industry along with other security documentation, certifications, and audits. Basically, you'll want to include everything a customer needs to evaluate your security posture.

Initially, this might seem like a lot of work, and it might take some time to pull everything together, but once you do, you'll save countless hours while also being able to reallocate members of your team to more strategic initiatives than responding to questionnaires.

Once you have all of your security documentation consolidated in one place, it's time to share it with your customers and prospects. Best practice is to share it at the very outset of the customer relationship to show you have nothing to hide. As mentioned previously, it's also a good way to build trust. But you shouldn't just share your security documentation with customers. You should also provide access to your security documentation publicly either on your website or on vendor security directories like the Whistic Trust Catalog or Cloud Security Alliance STAR Registry. Doing so enables customers and prospects to conduct Zero-Touch Assessments of your security posture.

Making security documentation available on-demand not only helps build trust with your customers, but it also makes good business sense. Whistic estimates that building a security profile and making it available on-demand could save you an estimated $43,000 in InfoSec labor costs that were once directed to responding to one-off questionnaire requests.

To help promote trust and transparency between vendors and their customers, Whistic, along with a number of top tech companies, including Okta, Airbnb, Zendesk, Asana, Atlassian, Snap, Notion, TripActions, and G2 formed the Security First Initiative. The primary goal of the initiative is to make vendors sharing their security documentation proactively the expectation for all businesses.

---

[1] 2022 Whistic State of Trust and Transparency
[2] 2022 Whistic State of Vendor Security

Trend # 2: Deepen integrations with procurement

As long as companies are onboarding new third party applications into their environment there's going to be a need for security reviews. That's why it's important to incorporate the security review into the procurement process, so it's not something that's tacked on at the end that slows a purchase from being made. When that happens it further lengthens the time it takes to get technology in the hands of employees that will help them do their job better.

Below are some logical workflows that when incorporated into your procurement process should speed things up without sacrificing the increasingly important security assessments.

1. Only finance can pay vendors. This helps secure not only your company's payment information, but it helps prevent rogue vendors from being added to the company environment without being properly vetted by procurement and the infosec team.

2. Requests for new vendors must be requested through the procurement system. When the request comes through the procurement system, you ensure both the procurement and infosec teams have everything they need to initiate the vetting process of potential vendors, eliminating the lengthy back and forth between requesters and procurement that used to occur.

3. Procurement determines if the vendor is approved or not. The next step may require a little effort on your part to integrate your procurement system with your vendor assessment software via API. This will make it easy for procurement to identify whether or not the vendor has been approved and passed a security review or whether a security review needs to be initiated.

4. Vendor reviewed and approved/ denied. If the vendor hasn't been approved by the infosec team, the next step is to kick off that process and once it's completed and the vendor passes, they can be added to the approved vendor list and the rest of the procurement process can begin.

Trend #3: Shift left

For those of you unfamiliar with what the term “shift left” means in respect of sales processes, it refers to the concept of moving the security review as early in the evaluation and development processes as possible.

For sales teams, this should happen at the outset of every customer engagement. In a perfect world, it would happen before the customer even engages with the business because that security documentation is available on-demand for companies to conduct security reviews on their own timeframe, as discussed earlier.

For engineering teams, it means getting security involved earlier and earlier in the development process to root out bugs before they become deeply embedded in the code and are difficult to remove. When you identify bugs early, it accelerates the process for fixing the problem and helps ensure that it doesn’t become a vulnerability that can be exploited later.

Shift left: The concept of moving the security review as early in the evaluation and development processes as possible.

Trend #4: From zero trust to zero touch

Moving forward, standard questionnaires and frameworks are going to continue to gain a stronger foothold against custom questionnaires that have become commonplace in recent years. When you dig deeper and take a closer look at most custom questionnaires, you will find they mirror questions and controls contained in standard questionnaires. If the goal is to just make the vendor jump through your hoops, that's counterintuitive to the vendor/customer collaboration we see as the future of vendor security.

Adopting standard questionnaires will simplify the process for infosec teams on both sides of the transaction. As we mentioned previously, vendors just need to respond to the questionnaires most relevant to their industry, package them in a Profile, and make them readily available to customers either by proactive sharing or by making them available publicly, which enables customers to conduct a Zero-Touch Assessment.

Making your security documentation zero-touch ready

For vendors, the first step is as obvious as it seems—assemble your security documentation. Based on Whistic data, the most commonly requested security documentation includes:

- Security white papers
- Security FAQs
- Privacy Policy

Other specific policies and procedures that may be requested include:

- Information Security Policy and Procedures
- Computer Encryption Policy
- Data Encryption Policy
- Data Flow Diagram
- Incident Response Plan
- Disaster Recovery Plan
- Privacy Policy
- Web Application Security Policy

The most commonly requested certifications and audits are, in no particular order:

- HIPAA Certification
- FedRAMP Certification
- Privacy Shield Certification
- PCI, SOC2, or ISO127001 Reports/ Certificates
- Pen Test Letter of Engagement
- Vulnerability Scan Results
- Other independent or third-party audit reports

There are tools available (i.e. Whistic Profile) that make it easy for vendors to build and compile all of this information into a format that is easy to publish to a trust page on your website or directories that house vendor security documentation. From there, buyers just need to seek out vendors that value transparency and conduct an initial assessment based on the information provided.

Trend #5: Real-time, current security and risk information

While security questionnaires are perfectly acceptable to conduct the initial vendor assessment, the information contained is only good for that point in time. A vendor's security ecosystem could change significantly in the period between assessments. That's why it's important to create a feed that is pulling in live information from various sources to ensure you have the most up-to-date information possible. Below are some tools we suggest integrating with your vendor assessment process to accomplish that goal:

- **Cloud Security:** Lacework, Orca, Whizz, Guard Duty, etc. These tools will help you automate cloud security and help you prioritize potential threats in your environment.
- **Phishing:** KnowB4, GoPhish, etc. Train your team about the dangers of phishing while also simulating phishing attacks to help them better understand what to expect in a live environment.
- **Compliance:** Drata, Vanta, TugBoat Logic, etc. Automate certification and compliance for SOC 2 and other certifications commonly requested.

Trend #6: Increased importance of Environmental, Social, Governance

Environmental, social, and governance (ESG) compliance and controls isn't a new concept, but more and more businesses are expanding beyond security and including ESG as part of their due diligence process.

These questionnaires are used to help companies consider how a vendor safeguards the environment, including corporate policies addressing climate change, for example. They also include social criteria to examine how the vendor manages relationships with employees, suppliers, customers, and the communities where it operates. The Governance portion of these questionnaires deals with a company's leadership, executive pay, audits, internal controls, and shareholder rights.

Whistic recently added the new SIG ESG questionnaire to its library of standards to help businesses streamline the process for vetting vendors based on this criteria.

Environmental, Social, and Governance: three key factors when measuring the sustainability and ethical impact of an investment in a business or company.

Trend #7: Transparency via Automation

Tools like the ones mentioned above can not only be utilized by companies trying to assess their security internally in real-time. It is also starting to be used by third party vendors to increase transparency with their customers to satisfy customer security reviews.

Vendors are figuring out the right balance between internal security and being transparent with their customers and getting more bang for their buck when they implement these tools. We are still in the early phase of this trend, but over time we will see more vendors thinking creatively about the tools they use and figuring out how to more effectively incorporate them into their vendor security strategies.

Trend #8: Moving from third parties to fourth parties and beyond

For companies looking to mature their vendor security program, a logical next step is to start delving into fourth party vendors that may touch your data. But when you move beyond third parties, the number of possible vendors to vet grows exponentially, so it can be hard to know which fourth parties you should actually care about.

To get started, the first thing you need to do is complete an accurate inventory of all your third parties, including type of data and volume of data accessed. Additionally, you'll need to have implemented an up-to-date risk rating methodology. Without these things in place, you'll have a hard time determining exactly what 4th parties to focus on. With that said, here are some tips to get you started.

Build fourth party awareness into the process. Include fourth parties in the questionnaires you send to the vendor, so they can inform you which fourth parties have access to data and be sure you have the ability to track critical fourth parties beyond the initial assessment.

Beef up your third party contracts. Make sure that disclosing fourth party information is included in the vendor process and that your third parties are required to ensure controls are in place for those fourth parties

Leverage your third party. While it's true that most fourth party vendors won't let you perform an assessment on them, that's why it's important to leverage the access your third party has with them. If you want any sort of due diligence on fourth party vendors, it's going to have to come directly from your vendor.

Be realistic. You shouldn't expect to be able to hold fourth parties to the same standard you hold your vendors to, but you should look for acceptable alternatives to a full-on assessment, like accepting a SOC 3 instead of a SOC 2.

How Whistic Can Help

Whistic was built to help vendors connect and collaborate with customers to ensure that relationships are built on transparency and trust. We accomplish this in three ways:

Enable proactive sharing. With Whistic Profile, vendors can compile all of their security documentation, including industry standard questionnaires and frameworks along with certifications and audits, into one centralized location. From there, vendors can proactively share their Profile with customers early in the sales process and publish to their website or the Whistic Vendor Security Network.

Facilitate Zero-Touch Assessments. Once the Profile is published to the Vendor Security Network, companies can easily search, find, and assess vendors without the time-consuming back and forth from the old method. Once they find the business they're looking for, they can access security documentation immediately and begin the assessment process.

Integrate with real-time risk management tools you already use. Whistic makes it easy for you to connect with tools like Drata that allow you to get real time risk information piped right into your vendor's Profile. This makes it possible to stay on top of changes in a vendor's risk posture in between assessments.

Learn more about how Whistic can help your business improve its vendor assessment process by **requesting a demo today at www.whistic.com/request-a-demo**

www.whistic.com