Security Questionnaires: A Guide for Information Security Teams

Sam Colt August 11, 2022

Naming the person responsible for security questionnaires at an organization feels like getting thrown into the opening scene of a murder mystery. Everyone is pointing at someone else in what feels like an endless stalemate. In the end, something or someone gives, but the results are usually ugly, to say the least.

Organizations are usually quick to charge information security analysts with the clean-up when a security breach happens. However, no one wants to take ownership of the various department inputs for Security Questionnaires beforehand, which could be crucial to preventing a breach in the first place. Why is that? Well, let's just say security questionnaires are kind of a pain in the a**.

A definitive security questionnaire process will reduce wasted time, increase team productivity, and ensure questionnaire completion. When questionnaires are timely and accurate, it means deals don't get stalled and even happen faster without putting the organization's security at risk.

What are Security Questionnaires?

Data security is a much more complex problem for organizations today. Gone are the days of a single internal data center. Behind each organization is now a network of SaaS tools, cloud storage, and outsourced services, each of which exposes your company and customer data. IBM Security reports that **14% of data breaches are a result of a vulnerability in third-party software** and **will cost an organization $4.33 million** on average. Which is where the "pain in the a**" security questionnaires come in.

Security Questionnaires are the first step in vendor risk management. They're a tool used to ensure that the partnership between an organization and a vendor will be sustainable and data and information exchanges will be secure. As much as they might be a pain to fill out, they're vital to safeguarding organizations in a digital enterprise landscape.

Each organization has its own type of security questionnaire based on its industry and operations. At the center of each is a similar objective, though. These questions are intended to reveal what safeguards (e.g., network security protocols) your organization or the receiving service provider has in place for data exchanges (e.g., confidential client records). This allows your organization (or the organization you're doing business with) to validate the safety of their business partnerships.

Anytime an enterprise deal is initiated, it should trigger a security questionnaire. Security Questionnaire responses are more than a way to verify security for an organization and its customers. They also dictate liability if the worst-case scenario happens — a security breach. For example, in the case of a security breach, a vendor that made false claims on a questionnaire can be held liable for damages.

If you're unsure how critical it is to vet your vendors and take proactive security measures, all you have to do is look at the data. According to IBM Security, the **global average cost of a data breach is $4.24 million**, with breaches in some industries like healthcare costing **as high as $9.23 million**. Whether you're receiving a questionnaire or requesting one, it's essential they're answered and reviewed with the utmost scrutiny.

> What is Security Posture and Compliance?
>
> An organization's overall state of security is summarized in what's referred to as the "security posture and compliance" of an organization. These safeguards can come in many forms: internal information security teams, software that prevents cyberattacks, internal policies that remove exposure to security breaches, and more.

How can information security teams streamline Security Questionnaires?

Security Questionnaires are often hundreds of questions long, covering everything from privacy policies to infrastructure for breach response and physical data server security. It can feel overwhelming to even know where to start for many Chief Information Security Officers (CISOs) and their teams. Even worse, enterprise deals can often be lost due to delays, inaccuracies, or not meeting the requirements of a questionnaire. So how can information security teams streamline the process on all fronts?

Compliance Frameworks and Certifications

There are many frameworks developed by different industries that are often used as baseline requirements for audits and enterprise architecture (i.e., how you structure your business to achieve end goals). Some of these frameworks can also be submitted by organizations in lieu of a security questionnaire or supplementary to a questionnaire.

If you base your security architecture on one of these frameworks and/or go through one of these frameworks ahead of time, it'll significantly shorten the turnaround on questionnaires. It does this by ensuring (a) you have the essential security protocols in place and (b) a clear correlation to the questions being asked (or even an already formulated answer). Here are some of the most common frameworks:

- **CIS Security Controls:** The Center for Internet Security (CIS) has a universal cybersecurity controls framework developed by volunteers from across multiple sectors. The controls are updated regularly via collaborative review by government agencies, industry specialists, and academia. This framework is broken down into 18 individual controls that cover different areas of organizational security.
- **SSAE SOC:** The Statement on Standards for Attestation Engagements (SSAE) Service Organization Control (SOC) report is a cybersecurity audit framework developed by the American Institute of CPAs (AICPA). This framework has two versions - SOC 1 and SOC 2.
- **CAIQ:** The Consensus Assessments Initiative Questionnaire (CAIQ) was developed by the Cloud Security Alliance (CSA) in an effort to provide security standards for the cloud industry as well as create transparency for organizations using cloud platforms. This security assessment is now combined with the Cloud Control Matrix (CCM) and covers Security Guidance for Critical Areas of Focus in Cloud Computing, the Security Trust and Assurance Registry (STAR), and a Code of Conduct for GDPR Compliance.
- **ISO/IEC 27001:** International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 standards were formed by a joint committee between the two organizations. They strive to cover a variety of industries, so the number of standards is quite exhaustive, and not all may apply to your organization. One of the major advantages of these standards is they're internationally recognized and exhaustive.

advantages of these standards is they're internationally recognized and exhaustive.

- **SIG:** The Standardized Information Gathering (SIG) questionnaire is published by the risk management nonprofit Shared Assessments. There are three types of the SIG: the basic SIG questionnaire (for initial vendor assessments), the SIG LITE (for low-risk vendors), and the SIG CORE (an extensive library of questions for IS teams).

- **NIST SP 800-171:** Like most government documentation, the NIST's full title is a mouthful, so brace yourself. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (*whew!)* is required by all federal agencies working with external vendors. However, this questionnaire can be used as a framework for non-government vendors as well. The process includes six steps: categorizing, selecting, implementing, assessing, authorizing, and monitoring.

These common frameworks serve as a map for structuring your security and answering Security Questionnaires. While they're a tremendous help, you still have to put in some work to reach your destination: a completed questionnaire. To make it easy on yourself, centralize all the answers in one place so you don't have to make constant detours along the way to find your answers.

Centralized Database for Answers

There are two main hurdles with Security Questionnaires: (1) they're so extensive, and (2) they often require input from multiple departments. As a result, Security Questionnaires often turn into the proverbial hot potato in an organization. They're passed around half-completed between departments, with each hoping the next will finish answering it, and somehow it'll end up complete. The easiest way to address both of these things is a database of answers. This way, stakeholders in each department can submit the answers that apply to their area. Then the IS team can easily find the answers they need when filling out various questionnaires and frameworks without trying to track down the right person in various departments.

> Note: These databases require regular manual maintenance to avoid data decay that could cause inaccuracies in your questionnaires. Don't have time for that? We got you! Set up a meeting today!

Proactive Communication With the Other Organization

Not all questions on a questionnaire may apply to your organization, or you may find you don't have the required security protocols in place. What then? The best way to address both of these problems is proactive communication with the sending organization. For example, if a question doesn't apply to your organization, proactively collect evidence for why that question is irrelevant rather than leaving it blank. This will assure the other organization that you're still a trustworthy vendor, and the proactive transparency will help build trust, which is really the purpose of a Security Questionnaire.

How do you answer a Security Questionnaire?

No matter how much you prepare, new security threats surface every day, and questionnaires can feel like a moving target. So how do you tackle such a massive undertaking? There are three primary processes for answering questionnaires: manually, automation through SaaS tools, or outsourcing to security specialists.

Manual Processing

Manual processes used to work fairly well before cloud services became so foundational for every organization. Now it's become nearly impossible to maintain information security and account for every questionnaire an organization is sent or receives.

If you use a manual process, IS teams are forced to painstakingly comb through questionnaires, hunt down answers, and hope they answered the questions in the way the sending organization needed. Or, if they're on the receiving end of a questionnaire, they have to comb through the responses as well as they can with minimal time and cross their fingers, hoping that they don't miss something.

In the digital age, with organizations exposed on so many fronts, internal teams have a hard time keeping up with the demands of the constantly shifting landscape. And, frankly, IS teams' skills are too critical to an organization to spend their time on questionnaires. IS teams can spend up to several weeks between teams to fill out a security questionnaire. In short, manual processes are not sustainable.

Automation Via a SaaS Tool

As teams have felt the weight of processing these questionnaires manually, they've turned to SaaS tools to provide automated reviews and responses. This has reduced some of the time processing on the front end, but unfortunately, SaaS tools are *only 50% accurate on average* and still take *seven days to complete* a questionnaire. Yeah, seven days. Enough time for that prospective deal to fall through. And that seven-day average doesn't even include the time it takes for the IS team to go back and fill in all the blank fields because the AI can't figure it out or find which 50% is done wrong.

Errors and blank fields aren't the only problems. According to SANS Institute, **48% of IT professionals** say a major risk to

Errors and blank fields aren't the only problems. According to SANS Institute, **40% of IT professionals** say a major risk to using these AI tools is the *lack of internal skills needed to implement them.* The lack of skills needed is arguably an even larger issue since the IT professionals also noted this is often unforeseen by the vendors of these tools. This means SaaS companies are peddling tools that not only don't solve your problems but are also not accessible for your team in the first place. Even worse? They're too out of touch to even realize it.

Partnering with Security Specialists

Outsourcing to security specialists marries the best of both automation and manual processes, plus adds even more value. Outsourcing to security specialists gives you the accuracy of a manual process without tying up internal teams. And outsourcing typically provides faster, more comprehensive results than either internal teams or SaaS tools.

One of the greatest advantages of having specialists work on your questionnaires is that they're well-informed of any changes or potential threats in the security space. This allows them to identify gaps your own team may not have noticed due to a lack of general awareness or of time. For example, you don't have to worry about if information about your SOC 2 review or last audit is up to date or not, they can proactively maintain that for you. Outsourcing Security Questionnaires is a great way to maintain a high-level security posture, as it's essentially an ongoing security audit by the most knowledgeable experts in the field.

It's Not Robots, It's the Yeti

We get that everyone is sick of filling out Security Questionnaires. Who has time on a Friday afternoon to answer hundreds of security compliance questions? What you need is someone who actually likes this stuff. Maybe a mythical creature like this exists. Maybe a yeti?

We love this stuff at SecurityPal. We have a whole team of security experts to make sure your questionnaires are compliant and timely. And we don't use random templates filled in by a robot. These are real humans painstakingly combing through the data, so you don't have to. And with the yeti, you know your questionnaires will meet the strictest security protocols since we've spent years studying Fortune 500, governments, and premiere companies. What does that actually mean? Well, we've processed over 80% of Fortune 500 security questionnaires, so we've pretty much processed every questionnaire in the universe. No big deal.

It's time for you to get back to what you do best — crushing deals (and taking that vacation you meant to take 5 summers ago). Ready to have all those questionnaires in your inbox in 24 hours? Check out what the yeti can do for you.