For many companies, the need to complete data privacy and security questionnaires are increasingly common. But they are also becoming longer, more complex, and a burden for the companies receiving them. We've helped companies answer hundreds of security questions for their enterprise customers — sometimes as many as 400 in a single questionnaire. In this Guide, we'll break down the basics of this effort, and provide a recommended approach.

Within this whitepaper, we'll cover ...

WHY ARE VENDOR SECURITY QUESTIONNAIRES SO PREVALENT?

Tech companies often receive, or send, written assessments to verify their company data is protected by businesses they work with. In 2016, the number of data breaches increased by 40%. It's increased every year since then and caused more companies to be more concerned about security.

A number of security breaches were also caused by smaller third-party vendors. Because of this, many companies are now sending and receiving questionnaires to record they have done due diligence on their technology vendors. Further, assessing the security of third-party vendors is often required by a company's own cybersecurity programs, government regulations such as GDPR, industry-specific regulations like SOX and NIST, and also cybersecurity insurance providers.

Over the past 5 years, the cost of a data breach has risen by 12% and now costs an average $3.92M!

As a result, we've seen an increase in vendor questionnaires in recent years, and they only get more intense as SMBs and startups in the supply chain are targeted by cybercriminals seeking to use them as an entry point into their enterprise customers. These questionnaires are especially common in the software service industry. That means both established software companies and SaaS startups alike need to be ready to respond. Your enterprise customers want to know what risks they are accepting by doing business with you.

VENDOR SECURITY QUESTIONNAIRES: A QUICK OVERVIEW

The title, structure, and length of these surveys vary widely. You might see them called a few different names, like a "Third-Party Assessment Questionnaire" or a "Vendor Cybersecurity Assessment." It could simply be a PDF titled "IT Security Questionnaire" and attached to an email. Or it could be sent to you as a link to an online form you need to fill out.

System glitches caused 25% of data breaches in 2019, and human error is the root cause of 24% of breaches

Depending on the company, these questionnaires may cover different topics including web applications, privacy policies, IT infrastructure, or physical datacenter security.

If a prospective client or existing customer sent you a security survey like this, your IT department could get it first. Or it might be in the sales teams' inbox. We've heard before how a team member opens a new questionnaire from a top client (or big prospect), only to panic when they face hundreds of questions about security.

In addition, you might also get questions about any of the following:

- List of cybersecurity policies
- Organizational security
- Physical security
- Communication operations and management
- Incident response and management
- Security by design
- Access control
- Etc.

5 STEPS TO RESPONDING TO A VENDOR SECURITY QUESTIONNAIRE

Okay, so you have the questionnaire in hand. You've reviewed it, and to be honest, you might be starting to hyperventilate a bit. There's a lot on here, and you're not sure if you even have all these policies in place. So, what now?

Don't panic!

We've helped many vendors answer these security questionnaires. On the next few pages, we'll give you tips on how to tackle it, how much time it's likely to take you, and what resources you'll need to respond to it. Here's how we'll "divide and conquer" to ensure success:

43% ... the percentage of all cybersecurity attacks that small businesses are targeted by.

1. Break down the questions
2. Identify specific security gaps
3. Recycle past security questionnaires
4. Understand the role of compliance
5. What to remember

Depending on the length and scope, you can expect to need to plan time from multiple team members to prepare your responses. It can be difficult and challenging. But more and more companies using technology from third-party vendors are scrutinizing the security of products and services they use.

While it will take time to answer the questionnaire, it will often take longer to become compliant if the vendor questionnaire exposed gaps in your security program.

You should plan not only to answer the questionnaire, but to also launch company initiatives addressing any issues it reveals.

STEP 1: BREAK DOWN THE QUESTIONNAIRE (AND THE QUESTIONS)

Reference your risk assessment ...

Before you answer a vendor security questionnaire, your company should have completed a risk assessment. This will help you understand the risks that may be involved for you as a vendor or your clients, setting the scope for what you need to answer in security questionnaires and what isn't applicable.

Then, you'll want to see if you can reduce the scope of the questionnaire. Start by scanning the list of questions ...

- How many questions are there?
- Does anything seem vague or need clarification?
- Do you know when they are expecting your response?

Clarify the questions ...

If you can narrow down the number of questions by marking some with N/A right away, that will help reduce the effort. You'll likely need to justify why it isn't applicable, but in many cases, the standard questionnaire will have questions that are irrelevant to the work you'll be doing with the company.

You may be able to identify specific areas that would affect your customer's data, ruling out multiple questions. Perhaps you don't store data locally, or there might be reasons that physical or network security doesn't apply to this engagement. Then you may be able to answer "NO" or "N/A" and offer a logical reason that you don't have this policy.

After weeding out any that are not applicable, you'll need to turn your attention to the rest of the questions. If something seems vague, mark it and ask the customer for clarification. While answering these questions, you'll want to break them down.

Let's take this example security question that you might see as a vendor:

> ***"Is there a Network Policy that has been approved by management, communicated to appropriate constituents, and an owner to maintain and review the policy?"***

The question may look fairly simple but there are actually FIVE parts to this question:

1. Is there a policy?
2. Was it approved by management?
3. Was is communicated to your staff?
4. Who is responsible for maintaining and reviewing the policy?
5. Can they see a copy of this policy?

If you don't answer or don't answer to their satisfaction, that can jeopardize your relationship with the customer or disqualify you from their list of software vendors. But breaking down a question into parts will help you see which parts you have and identify any gaps.

STEP 2: YOU LACK SPECIFIC SECURITY CONTROLS: NOW WHAT?

You might be able to answer "YES" to everything. You might have comprehensive policies, procedures, a training program for employees, and a robust InfoSec program.

If you are using an information security platform, you'll easily be able to report on your existing policies and demonstrate adherence to them, as well as map your security controls, which allows you to assess your own program against major frameworks like the CIS, CSC, and SOC 2.

On the other hand, you may have to answer "NO" to items that you do not have covered. If you only have a handful of policies that don't cover all these topics, you should look into updating your security policies.

If your company needs to upgrade a security program, you may be able to use policy templates or tools that can generate and track your policies, implementation, and build out your information security program.

Missing Security Remediation Plans?

You may be able to show a remediation plan which will bring your product or service up to your customers' security standards within a set timeframe or by the time a new engagement starts. This is especially important if you can't reduce the scope of the questionnaire or complete a risk assessment ahead of time.

Your remediation plan should show that you have a process to work through any gaps exposed by the questionnaire. This shows you are doing your due diligence and taking their concerns seriously. You want to keep your customers in the loop about your security compliance.

This open communication about how you plan on implementing security upgrades can go a long way to building trust. It also shows you are taking responsibility and moving in a positive direction. Be honest and open about your level of

security or you risk exposing yourself and business to serious consequences. Don't be dismissive. Take responsibility for any security gaps. If you are in the process of creating new policies and implementing security controls, ask the customer if you can complete the questionnaire after those new controls are in place.

Finally, while there are a number of great and smart answers you can provide when answering a vendor security questionnaire, there are also some not-so-good (perhaps terrible) answers you can provide, as well. This includes the following ...

1. ***"My CTO (or some other person on our team) is pretty good with security and I know he does a bunch of stuff."***

   Yes, it is absolutely a good thing to have *someone* on your team with security knowledge and experience. However, there are two significant problems with this common statement.

   First off, if the person you are referring to is the most knowledgeable and is actually doing the security work for your company ... why is that person not the one responding to the questionnaire?

   The next issue here is that the business leaders who say this are outright admitting that they have no idea what things the security person is doing. That means they are not mandating security from the top down. They are not seeing reports on security operations. This is like telling the auditors that you don't know and generally don't care. If you aren't aware of your own security procedures, that's a sign that you need to start building a new cybersecurity program.

2. ***"We are in AWS and all of our email is in Google."***

This is the most common statement we hear. Allow me to translate this to what it means to a security professional: "*I am completely naive and don't know anything about securing my company or your data. I genuinely believe that because we are in the cloud, using industry-leading cloud applications and infrastructure, I can rest easy and not worry or even think about security.*"

Let me clarify. Yes ... cloud-based services like Amazon Web Services (AWS), Asure, Microsoft 365, and Google all have world-class security programs to protect their customers and their data centers. But you can't rely exclusively on their security to protect your data, your web application, or your customers' data. On a sample of over 100 pen tests conducted last year on AWS-hosted web applications, affiliated pen testers were able to take control of the application and download entire customer databases 40% of the time. AWS wasn't at fault: it was always the fault of the startups that were tested.

Yes, it is critical that you work with secure web apps and hosting companies. However, it is just as critical that you implement proper secure coding, testing, access control, and auditing practices. At the very minimum. Without that, your web application is at an increased risk of a cyber-attack. When a vendor security questionnaire (or an auditor, for that matter) asks about the security of your application or your security posture and you spit out an answer like this, your risk profile goes through the roof. A poor cybersecurity posture can quickly damage relationships with existing customers or new sales.

3. "***We are a startup and don't have the time or money to deal with antiquated policies and procedures."***

I hear founders say this with surprising arrogance. Sort of like, "*We are cool and move fast and creatively, so we are not a bogged-down, red-tape-induced slug like your organization.*"

The person(s) reviewing your security questionnaire probably won't find that attitude very amusing or reassuring, but that is not the worst part. This statement demonstrates that your primary concern is running out of money and going out of business. From the customer's perspective that introduces another risk that may need to be focused on: what happens to users' data if this startup goes belly up?

You have to make the time. You need to find some money. You can also access a multitude of free resources to help to secure your business. Even with free resources, you also have to be proactive and care about your security to use them effectively.

4. ***"We have some policy documents in a folder so I will dig them up and see if we have what you are looking for."***

Generally, when I hear this statement, this is how I interpret it: "*We don't have anything, but if you really need something we will pull an all-nighter and put something together using some templates from the internet. We don't care much about security.*"

If you actually are not lying, then you are at the very minimum saying that you are not aware of what policies you have. You don't even know where they are stored. You are showing that you do not really care about them. That means nobody else in your company cares, which means these policies are not being followed and serve no functional

purpose. They're probably in desperate need of an update.

If you *actually* had policies and you *actually* cared about security and you *actually* followed them, then you would be able to respond to this question. Be ready for this question. You should have a reasonable and informative answer about your security policies. Maybe it sounds boring, but policies and procedures are foundational for your security.

5. ***"We do some internal pen testing on our application."***

This is usually a response to a question around penetration testing. When auditors ask you about pen tests, they are likely referring to an actual pen test conducted by an experienced and certified third-party pen tester.

There are three key concepts that are critical to a pen test being considered valid:

1. Is it a *real* pen test? Unfortunately, the term *pen test* is often misused referring to a *vulnerability scan*. They are not the same. Running a vulnerability scanning tool like Nessus on your application, although good practice, is not a penetration test. That is simply a scan that looks for known vulnerabilities.

2. Is it a professional pen test? Pen testing is not the type of thing where you read a few blogs and then you are a qualified pen tester. It is a career, and there are people who are really good at it. They get this way by reading, studying, and, most importantly, practicing.

3. Is it a third-party pen test? A pen test conducted by the same person or people who are building your software is very biased. Can you trust them to honestly disclose a major security vulnerability in the report they send to you, their prospective customer?

A third-party pen tester's reputation and career depend on the credibility of their pen tests. A CEO's career depends primarily on the company's ability to close business and hit revenue targets. If your company can't pass pen tests and a security audit, those are troubling signs you won't be able to close deals with enterprise-level customers.

6. ***"We don't store any confidential information."***

Now, if this is actually 100% true, then this may be a good answer. However, what we see over and over is people saying this, but then as we dig deeper, we realize that they store personally identifiable information, user habits, insinuated data, and data that is regulated by one or more privacy or security regulations.

When you say that you don't store confidential or sensitive information as an answer (or excuse) for your lack of security and then the auditor figures out that you actually do, you are in a really bad spot. Basically, you are completely lying to try to get through this questionnaire, you are not aware of the data your company stores or processes, or you are completely unaware of what is actually considered regulated or sensitive data. OR All OF THE ABOVE! Whatever the case, this attitude rapidly erodes trust and will likely kill a deal with any security- and privacy-conscious customer.

STEP 3: RECYCLING ANSWERS FROM PAST SECURITY QUESTIONNAIRES

Typically, you can't reuse a security questionnaire. But that will depend on the customer.

If it seems like it might be an option, you may want to ask first. In most cases, they will have a customized questionnaire. If you offer the customer a generic, completed security questionnaire, you should expect that they will have additional follow-up questions. They may still ask you to answer the original questionnaire if it is a requirement of their own policies and procedures.

However, you should certainly keep any of your completed questionnaires on file. This will allow you to reference past answers and reuse the relevant parts for a new customer's questionnaire. Companies will often find that answers change, so you will want to make sure you are offering the most updated information about any recent security upgrades.

Questionnaires will often have topics that overlap. Keep track of what security questions you've answered. You may even want to create a central repository of your responses to different questions about your policies and procedures for later.

STEP 4: HOW COMPLIANCE WITH A KNOWN FRAMEWORK CAN HELP

Whether you can use a certification of compliance in place of a questionnaire will also depend on the customer and their questionnaire. Although holding a certification or proof of compliance will definitely show you are taking security procedures seriously. However, they may still have questions that are not addressed by a certain framework or relate specifically to their business.

If you have a report from a security management tool, it is possible that they will even accept that in lieu of the questionnaire

Compliance with a popular security framework will ultimately help you to answer the questionnaire. Many of the topics required for certification or compliance will be covered in the questionnaire, preparing you to address those sections. If you have documentation about compliance with SOC 2, ISO27K, NIST, or CIS, that will give you an advantage while you respond to the questionnaire. These also provide outside support about your security measures.

STEP 5: WHAT TO REMEMBER WHEN YOU'RE ACTUALLY FILLING IT OUT

Keep it simple. If the question is straightforward and can be answered in a single sentence or a short paragraph, do that.

Only provide the information required by the question. If the customer doesn't ask, don't overload them with information. More information can also create issues during the review process. The customer is responsible for asking for more details if they need them.

Be self-aware of both your strengths and weaknesses. Don't lie (or even "stretch the truth")! Don't overstate your security controls. And don't give them excessive justification or excuses for why you lack specific security controls.

Involve the right people. Assign people from your team who know the answers to these questions. In some cases, this means taking time from a lead engineer or even a CIO/CTO. If you need to, divide the questions and spread the responsibility across several people

Keep the lines of communication open. Confirm you received the questionnaire. Share security documentation you have, particularly if you have a security platform that can produce reports on the state of your Infosec program.

Request more time to complete it if you sense it will be challenging for your ream. Ask for clarification. And also look for outside resources to address lacking policies or increase your security compliance.

Take your time. It might take 8 hours; it might take 20 hours; it might take even longer. We've seen instances where it has taken days to complete or drag out for weeks while a vendor and customer go back and forth clarifying questions. You want to get it right, so don't rush it!

WHAT QUESTIONS (THEMES) TO EXPECT FROM VENDOR SECURITY QUESTIONNAIRES

We've assisted our customers with answering many cyber security questionnaires. Here are some examples of common "themes" you might expect customers could ask you:

1. Is there an Information Security program in place?
2. Do you have an approved and published set of Information Security Policies? Is there senior management oversight and approval of the InfoSec Program?
3. Do you have an identified individual who is responsible for Information Security?
4. Do you screen your employees for criminal or financial irregularities before and/or during employment?
5. Is there senior management oversight and approval of the InfoSec Program?

CONCLUSION

Many small and mid-sized businesses are most at home working within Microsoft Word or spreadsheets. But with security policies and questionnaires becoming ever more complex, you'll want to make sure your team looks at how you can optimize and streamline your processes by using tools and/or processes designed for the job.

Having trained and experienced cybersecurity professionals available to you can reduce an organization's stress in completing vendor security questionnaires exponentially ... and this is exactly where CISO ToGo, LLC can help!

If you'd like to discuss exactly how we can help, get in touch or visit us at:

www.CISO-ToGo.com

Locations: throughout the United States

Email: **WRichmond@CISO-ToGo.com**

Phone: **401-264-0880**

CISO ToGo
Technology Risk Consulting

because security is everyone's concern, but it's OUR business!