Why Cyber Security Questionnaires Are Making Or Breaking B2B Sales

Contents

SECURICY

Introduction

Answering a cyber security questionnaire is an enormous hurdle for many small businesses. Failing to show adequate understanding of the risks can jeopardize sales to enterprise-level customers. But for small businesses that are ahead of the curve this is also a competitive opportunity. Businesses with a cyber security program have the advantage of quickly assuring customers they are a safe vendor.

New cyber security assessments are slowing down or killing sales deals for small and medium-sized businesses. Especially businesses that sell online services to enterprise-level companies.

More and more companies are sending out these cyber security questionnaires, which dig into the privacy and data security of potential vendors. Big box stores, financial companies, and government agencies have sent these questionnaires out for several years, but now more small businesses are following suit. At Securicy, we've even seen 10-person companies send out cyber security questionnaires to vendors.

The Questionnaire That Can Kill Deals

Let's say you're the CEO of a small business-to-business marketing company. You sell a software-as-a-service product. You have a big deal coming down the pipeline, an opportunity to bring on the largest enterprise customer your small company has ever had.

Then Brandy, your contact at the prospective customer, sends you an email. Brandy's procurement department requires all product vendors to complete athis security assessment. Their attorneys and insurance carrier need it. Her email has an attachment with almost 100 questions digging into your cyber security protocols. Your background is in B2B sales and you have no idea what most of it means.

You panic.

Your team tries to answer all the questions. But the whole deal falls through. The biggest opportunity your company ever had is gone.

Then... the next customer sends a questionnaire.

Why All The Questions About Cyber Security In A Sales Cycle?

This kind of scenario is becoming all too common. Businesses risk losing sales because they don't have good answers and explanations about their cyber security posture. Or worse, they have no cyber security protocols and discover their entire business is wide open to attacks.

If a B2B company has not gotten a questionnaire yet, it's only a matter of time until it happens. Cyber attacks are increasing damage to companies and raising security standards.

Confidential company and customer data need increased protection as businesses integrate more technology and online services into everyday operations. Tech and software businesses, even small teams, are at a high-risk of being targets of cyber attackers. Especially if those small teams work with Fortune 500 companies.

The costs of cyber attacks and breaches are high. Business disruption. Stolen information. Damaged equipment. Loss of revenue. These high costs force a business to scrutinize every third-party vendor that could increase their exposure to cyber attacks.

One malicious attack can cost a big business millions of dollars and take months, weeks to resolve. Large companies spent an average of $2.5 million and 50 days to resolve a single malware attack in 2017, according to data collected by the consulting firm Accenture.

Every year we see an increase in new hacks, malicious code, email scams, compromised secure networks, unauthorized downloads, and other cyber attacks. Big businesses are putting more and more pressure on their vendors to prove privacy and security compliance.

Businesses of all sizes are sending out cyber security questionnaires now. Before every new contract, they use the questionnaire as a tool to investigate potential vendors. For a CEO selling business-to-business products, this can drag out the sales cycle and kill deals. Businesses are evaluating the security measures they have or should have. They need to identify what critical protocols they are missing. Then they must ask all of their

vendors to do the same.

Not to worry, you can prepare for this questionnaire. You can handle it with professionalism. You can assure prospects that you have a cyber security program in place. All this helps set your company apart from the competition and close deals faster.

What To Do When The Questionnaire Hits Your Inbox

For a small business, answering pages and pages of technical questions is a major undertaking. At Securicy, we've seen as few as 10 questions and as many as 148 in a single questionnaire.

But there are actions you can take to prepare before the questionnaire lands in your inbox.

Securicy's CEO, Darren Gallop, recommends four steps for every company with a new cyber security questionnaire in their inbox. Read it. Set up a clarifying call. Answer the questionnaire. Then set up a follow-up call.

1. Read the entire questionnaire

Before you answer a single question, Gallop says your CEO, CTO, or knowledgeable team members should look over the questionnaire. Your team needs a high-level understanding of how in-depth the questions are. Mark questions you can easily answer. Note questions you need to research and discuss with your team. Flag questions that are unclear or don't seem applicable to your business.

2. Ask for more information

Before sending back any of your answers, set up a clarifying call. The primary objective of this call is to get a sense of the company's objectives with the cyber security assessment. Your aim here should to gain an understanding of their their goals? You should work to get a sense of how stringent their cyber security standards are for vendors? Are they flexible on some answers? What is their timeline to get the questionnaire answered? Will the answer get reviewed by attorneys, insurance professionals, or a security team?

Gallop says that in the conversation you can find out how closely the potential customer will examine your answers. It also demonstrates your cyber security awareness. Some businesses just want to satisfy their insurance carrier by collecting a questionnaire, but others have experts who will scrutinize it. Once you understand the situation, you can move forward with the questionnaire.

3. Answer the questionnaire

After a clarifying call, you may have some questions you can simply answer with "not applicable." This helps to narrow down the number of questions you need to address. Some questions need a simple "yes" or "no" answer. Others require explanation, diagrams, or documentation from previous security audits.

In some cases, if a business has few cyber security protocols, the questionnaire could expose broad risks to customers or partners.

Depending on the timeline and customer's requirements, you may be able to implement some policies before the contract begins. By engaging with the customer, you may be able to define and satisfy their needs to get the contract signed.

4. Set up a follow-up call

After completing and submitting the questionnaire, plan for another call. During this call, you can address any final concerns and clarify issues that need more detail.

If there are any problems, you can be proactive about finding solutions that will satisfy your customer. Businesses with serious concerns about data breaches and security will appreciate your efforts.

5. Incorporate lessons learned into your security program and sales process

Make sure you take issues identified in a questionnaire, or that caused a deal to fall through, and utilize that new information.

If you found critical cyber security components your company is missing, now you can address the risks to your own company and customer data. You can take steps to protect your own company and assets.

Implementing missing policies and programs can make sure the next deal won't hit the same roadblock. Some companies incorporate answers to common cyber security questions into their sales materials. You can sometimes avoid a questionnaire by giving a customer a one-page security document during the sales process.

It's also important to keep an eye on relevant events and new regulations. Laws and regulations can have a broad impact on small businesses. For instance, businesses with customers in Europe must comply with the General Data Protection Regulation (GDPR). It's important to know what kind of compliance you and your customers are subject to.

How Not To Answer A Questionnaire

You should never lie on a security questionnaire. If a company discovers a data breach was a result of a vendor, and the vendor lied, there could be dire consequences. Lying about security measures can result in severe legal action, bankruptcy, or criminal charges. Stolen information can seriously damage a business. In severe cases, criminal charges can reach as far as insiders with knowledge about the issue including company board members.

Trying to obscure or fake security protocols can also harm a business relationship and reputation. Beyond that, a business that takes the questionnaire lightly will lose trust and credibility with a customer. Dismissing or glossing over important security issues will only damage future sales. In addition to leaving your company open to cyber attacks.

In a landscape where threats are increasing year after year, security is essential. In this environment, small businesses that handle cyber security questionnaires professionally will have an advantage with enterprise-level sales. All while protecting their own business and assets.

Example Questions

Here at Securicy, we've assisted our customers with answering cyber security questionnaires. We collected some examples of questions customers could ask about your cyber security policies and implementation.

1. Is there an Information Security program in place?

The company wants to see that you have policies, employees have read them, and you have a plan for data security.

2. Do you have an approved and published set of Information Security Policies?

3. Is there senior management oversight and approval of the InfoSec Program? Give details if possible.

4. Do you have an identified individual who is responsible for Information Security? Give details if possible.

In Europe, this is often called a "data protection officer." In smaller companies, an executive such as the COO or CTO may be designated to fill this role.

5. Do you screen your employees for criminal or financial irregularities before and/or during employment? Please provide details (e.g. Reference, Criminal Record, Finance, etc.)

Here at Securicy, we have seen companies go so far as to ask to do their own background checks on a third-party vendor's employees. In some circumstances, the vendor can successfully negotiate a compromise to avoid unnecessary cost or burdens on the company and employees.

6. Have you implemented data classification? If so, provide details.

7. Are external security audits conducted on a regular basis?

A penetration test is the most common method. Many developers don't consider security as they push out products and features, but waiting until a product is complete to integrate security measures can incur massive costs. The threat of an annual penetration test can help ensure your developers consider integrating security measures.

8. Does the third party vendor have a defined software development lifecycle (SDLC)?

This shows if your team uses a security software methodology, such as the Open Web Application Security Project.

Conclusion

The number of cyber attacks and data breaches has escalated at an alarming rate. In response, standards for cyber security and data privacy have evolved. Answering a cyber security questionnaire is an enormous hurdle for many small businesses. Failing to show adequate understanding of the risks can jeopardize sales to enterprise-level customers. The good news is companies that focus on security and implement compliant data security practices can be ahead of the curve, gain competitive advantage and win more business.

About The Authors

Darren Gallop is a technology entrepreneur and a cyber security specialist. He is co-founder and CEO of Securicy.

Shannon McFarland is a content strategist, writer, and former journalist focused on telling true stories about good ideas.

About Securicy

Securicy is a quick and effective cloud-based service that customizes security program implementation. Our customers are fast-moving teams that need cyber security that fits their culture and skills. They serve clients that adhere to strict compliance standards. Securicy's policies and procedures engage and empower entire teams to protect their clients data. Securicy delivers strong cyber security posture as a competitive edge that translates into our customers winning more business.