www.whistic.com

HOW TO BUILD A **PROACTIVE MODEL**

for Responding to Vendor Security Questionnaires

whistic

CONTENTS

INTRODUCTION

In the world of monitoring and managing third party security initiatives, it's no longer sufficient to do the bare minimum.

Of course, remaining compliant and meeting guidelines will always be important, but there needs to be more focus on the actual process for both your vendors and your internal InfoSec team.

As more and more vendors turn to the cloud for operations and hosting, having a robust security questionnaire strategy in place is only becoming more critical. With so much data stored in the cloud, especially when it comes to IT/InfoSec, vendor partnerships are constantly at risk. The average cost of a data breach is $3.86 million, and this number is only growing: according to Soha Systems, 63% of all data breaches can be linked either directly or indirectly to third parties.

$3.86 M

average cost of a data breach

(& growing)

63%

of all data breaches can be linked to third parties.

according to Soha Systems

So, what should this growing dependence on third party security tell us? That managing third party security, responding to questionnaires, and tracking security data needs to be a top priority for IT/InfoSec teams. And, in order to do this job seriously and mitigate risk, IT/InfoSec departments must have the right tools and solutions in place to ensure nothing slips through the cracks.

As we go through the old model of third party security, it's not hard to notice a distinct pattern: the first three steps for an IT/InfoSec team are completely reactive! The new model, however, thrives on **proactive data, automation, and a forward-thinking strategy.**

Today, most third party security questionnaire reviews are handled in a chronological order. That is, when a questionnaire comes in, it kicks off a step-by-step process that, unfortunately, is repeated time after time as new questionnaires come in. The step-by-step mentality of many security questionnaires occurs organically due to internal roadblocks and processes. While many teams try to manually automate the process, the very nature of security questionnaires has long dictated that this information should not be stored or saved in any manner. But, luckily for IT/InfoSec teams, there are actually innovative ways to streamline the third party questionnaire process and develop a proactive security strategy.

In this ebook, we'll walk through the phases of **building out a proactive third party security questionnaire response process,** starting with reactive data gathering process and ending with a fully automatic, secure security profile that is ready to share directly with vendors.

PHASE
1

INITIAL COMPANY-WIDE PANIC

When a questionnaire request first comes in from a third party vendor, there can be a permeating sense of panic that ripples throughout an organization

It often becomes an 'all-hands-on-deck' situation for executive leadership since these questionnaires can vary so much in content and direction. While InfoSec team members and CIOs might feel like the questionnaire lands squarely on their shoulders, it's actually a company-wide initiative, and should be addressed as such.

To set your team up for success, don't panic! If you're dealing with your first questionnaire (or your first in a long time), then it might be worth your while to have a quick executive team meeting. Review security best practices and make sure other department leaders understand what will potentially be required of them down the road.

Keep calm, and start getting organized

PHASE 2

INTERDEPARTMENTAL COMMUNICATION

Once your executive team is in the loop, it's time to determine the actual content needed for your questionnaire.

There are a few different departments a questionnaire might involve, depending on the type of vendor and the nature of your partnership:

- **IT and/or InfoSec:** handles all technical aspects, including integrations, APIs, etc.
- **RFP/Marketing:** for any branding, messaging, or product marketing details
- **Sales:** if there are any joint customers or lead sharing details involved
- **COO:** for executive guidance and visibility into questions and answers

Regardless of the departments you pull into your questionnaire discussions, it's important to discuss and delineate these responsibilities early on in your security review process. This way, as you move forward and build a more robust pipeline of vendors, everyone is on the same page as to what team is responsible for which data points.

It's important to discuss and delineate responsibilities early on in your security review process.

PHASE
3

KNOWLEDGE BASE CREATION

For IT/InfoSec team leaders, the sheer amount of data required for a vendor security questionnaire doesn't have to be repeated

Just think: the average company's network is accessed by 89 different vendors every week, and every single one of these organizations requires a vendor security assessment. Simply put, this is a ton of data.

Typically, when a security team is faced with a questionnaire (and after phase 1 and 2 in which various other teams are consulted and involved), the following workflow plays out:

1. The team member in charge of filling out the questionnaire (usually a CIO, CISO, or IT Director) receives the questionnaire.
2. He or she then proceeds to comb through dozens of content documents where other team members have compiled their input and answers to previous questionnaires.
3. The person in question can spend days (or even weeks) sorting through Google Drive, Sharepoint, or other systems like Confluence searching for the right answers to all of the questions.
4. The questionnaire is completed and returned.
5. Another questionnaire appears and the process starts all over again.

The above workflow (and the data gathering from phase 1 and 2) is too reactive of a process t**o be scalable and accessible in today's modern InfoSec environment.** The knowledge base required for today's vendor security questionnaires are too complex and too dense for one person to manually comb through and fill out.

The average company's network is accessed by 89 different vendors every week.

PHASE
4

EVENTUAL REALIZATION

After experiencing the stress of a security questionnaire multiple times, most organizations are quick to realize their team needs a systemic, scalable solution to conduct security reviews.

Sometimes, teams turn to multiple disparate products and systems to try to band-aid the real issue at hand.

The transition point between simply doing it and realizing there is an unnecessary step in the process occurs when a team realizes exactly how much time and resources have been spent (and, in some cases, wasted) on responding to security questionnaires. Soon, questions are repeated and trends begin to emerge, making manual responses just seem silly and imprudent.

Sometimes, teams turn to multiple disparate products and systems to try to band-aid the real issue at hand.

PHASE
5

INTRODUCTION OF PROACTIVE SOLUTIONS

Once teams have moved on from manual solutions (goodbye forever, Box, Google Drive, and more!) they're ready for proactive, automated solutions designed specifically for vendor security


matterport
whistic
CASE STUDY
SECURITY PROFILE™ IMPLEMENTATION
With Whistic's robust platform streamlining their security questionnaire response process, Matterport has saved time, resources, and money. A summary of results to-date include:
An ROI of nearly 10X
INCREASED CUSTOMER SATISFACTION
AN ANNUAL COST REDUCTION OF 90%, SAVING OVER $50,000 PER YEAR WITH WHISTIC COMPARED TO MANUALLY PROCESSING SECURITY QUESTIONNAIRES
Deeper customer insights into how accounts are engaging with security review documents
A DECREASE IN AVERAGE SECURITY REVIEW TURNAROUND TIME FROM 4 weeks to 1 day
Shortening the sales cycle by nearly at least one month on deals with a security review has enabled sales reps to have more capacity to close additional business
"Just the other day a comment came in from a customer about Whistic. He emailed me and said, 'Thanks for setting this up! This is a really helpful tool.' This just goes to show how Whistic is increasing security satisfaction for both our internal team and our customers. We are excited about the future with Whistic and look forward to leveraging the platform in new ways."
SIMON WYNN, SVP OF SOFTWARE ENGINEERING AT MATTERPORT
CASE STUDY // MATTERPORT 1
WHISTIC.COM

As an IT/InfoSec leader, simply filling out a questionnaire once and then sharing those same answers with countless other vendors. Leveraging a secure platform to house your vendor security questionnaire answers (from across different teams and departments, no less) can allow anyone from sales to IT/InfoSec to confidently respond to security questionnaires.

Now, you might be thinking that a standardization of security questionnaires isn't possible because of custom NDA agreements that are associated with security reviews. If you're using a solution that is custom-built to help IT/InfoSec teams operate more efficiently, your team can send and receive custom NDAs without worrying about data integrity or risk.

Leveraging a secure platform to house your vendor security questionnaire answers can allow any role in your company to confidently respond to security questionnaires.

DEVELOPING A PROACTIVE SECURITY RESPONSE PROCESS

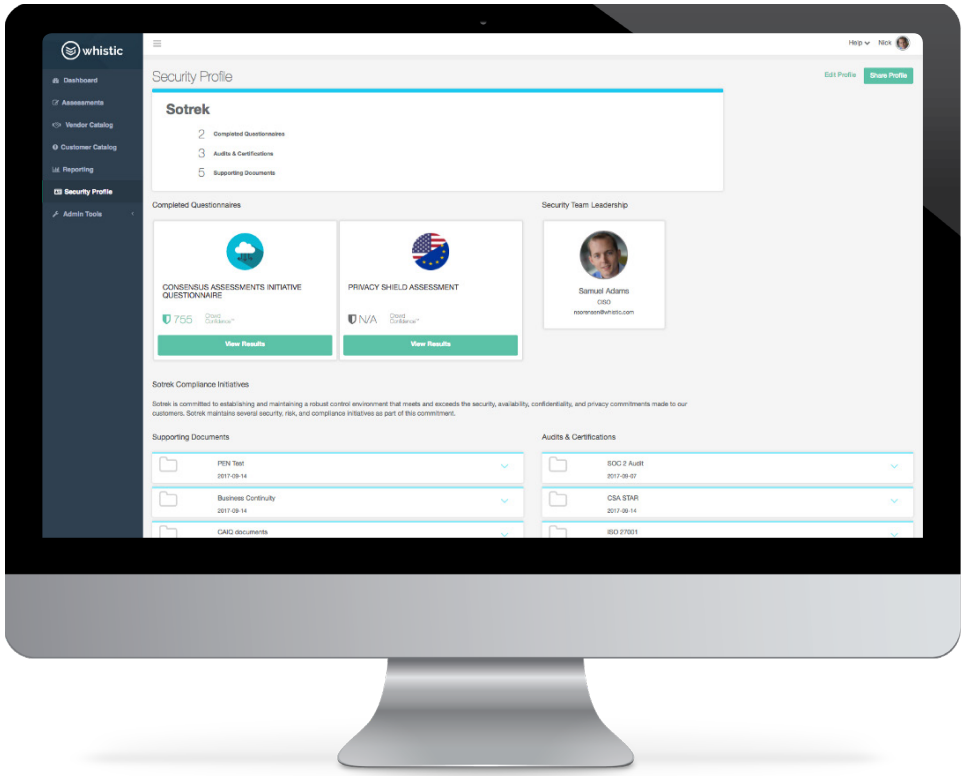
Building and maintaining a long-term security response process sounds like a tedious process, but there is a light at the end of the tunnel.

For teams that are truly dedicated to scalable solutions and delivering a more streamlined questionnaire experience to their organization, skipping phases 1 through 3 is possible. There really isn't a better time to invest time and resources into an updated vendor security questionnaire management platform. According to the 2018 Ponemon Report, **leveraging security automation can decrease the cost of a data breach an average of $1.55 million.**

With Whistic, the industry-leading security profile platform, teams can now:		
Proactively prepare for security requests with an easily accessible, organized knowledge base	Save time and resources by replacing manual processes with intelligent, automated workflows	Increase signed deals with new clients by getting completed questionnaires back faster

So how does it work? The Whistic platform automatically standardizes your knowledge base for immediate use across all security questionnaires. When a vendor requests a security review, your team can deliver a fresh, dynamic professional profile that is up-to-date and ready to be reviewed. The best part? Whistic works with companies of all sizes who are having issues or roadblocks in their security questionnaire process.

If your organization is ready to compete in the modern world of IT vendor security, then it's time to move to the new proactive model of vendor questionnaire responses.



ABOUT WHISTIC

Located in the heart of the Silicon Slopes in Utah, Whistic is a leading third party security assessment platform. Built for information security teams looking to improve the effectiveness, efficiency, and scope of their third party security assessment program, Whistic enhances productivity and unlocks insights traditionally trapped in staticsecurity questionnaires. Using the platform's intelligent and automated recurring assessments, Whistic customers eliminate the administrative burdens of back-and-forth third party requests and free up time to focus on security. The Whistic platform is designed for an intuitive and collaborative user experience and harnesses the wisdom of hundreds of security professionals to deliver risk insights through its proprietary CrowdConfidence™ scoring algorithm.

For more information, visit our website, read the latest on the Whistic blog or follow Whistic on Twitter.

whistic