WWW.WHISTIC.COM

WHY THIRD-PARTY SECURITY IS CRITICALLY IMPORTANT

5 Things You Can Start Doing Today to Build Awareness with Your Executive Team

whistic

CONTENTS

INTRODUCTION

You've been there before: you're in a meeting with an executive at your company discussing priorities for the security team in the coming year and making a case to allocate additional budget to your team. When third-party security comes up, the discussion somehow focuses on meeting the minimum requirements in order to maintain compliance with your upcoming audits. **The message so often communicated by executives in these meetings is that the Information Security team needs to do whatever it takes to ensure the company meets audit and compliance guidelines in order to allow the company to continue to add new customers at an increasing rate. A negative audit result or failure to maintain compliance with a standard could damage the reputation of the company.**

But what could damage the company more than a data breach that exposes your customer records? What about a discussion on the security of your data instead of just compliance with audit requirements? You bring up third-party security with your executives and explain that the company shares data with vendors and partners that are outside of the scope of any audit, some of which have never been reviewed. You ask for additional resources to be able to expand the scope of your security assessments so that you can review each new vendor and perform ongoing assessments of existing vendors. Perhaps you even discuss a request to add a new member to your team that can focus on understanding which vendors and partners have access to which types of sensitive data and what their security posture looks like.

But this somehow doesn't feel like a priority to your executive team.

INTRODUCTION

After all, when was the last time your company had a data breach? That's something that happens to other companies, not yours, right? And if there is a breach, it's certainly not because of some software tool that one of our business units purchased last year. To executives, third party security may seem too much like an insurance policy that your organization will never use. This means that they would rather focus security resources on 'more pressing' matters with results that can be easily demonstrated, such as responding to security-related RFP questions from potential customers and partners.

This shouldn't be the outcome of the meeting considering that in 2016, the number of data breaches increased 40%, with the average U.S. data breach costing $7.1 million. On top of that, consider the astounding fact that 63% of data breaches are linked to third parties in some way.

The Rapid Adoption of SaaS

Where does this increasing need to assess third party vendor risk come from and why is it more important today than ever before? Well, as any Chief Information Security Officer knows, cloud infrastructure and SaaS products are entirely taking over the landscape of the technology industry. Every time your organization puts data in the hands of a vendor, it raises concerns about the security of that data. According to IDC, the Software as a Solution (SaaS) market is growing at 5X the rate of on-premise software adoption, which increases the risk of an incident every single day.

A Gartner article estimates that over half of new large-enterprise application adoptions in North America will be composed of SaaS or other forms of cloud-based solutions. Additionally, predictions estimate that by 2019, more than 30% of the top 100 largest vendors will be shifting software priorities from 'cloud-first' to 'cloud-only.'

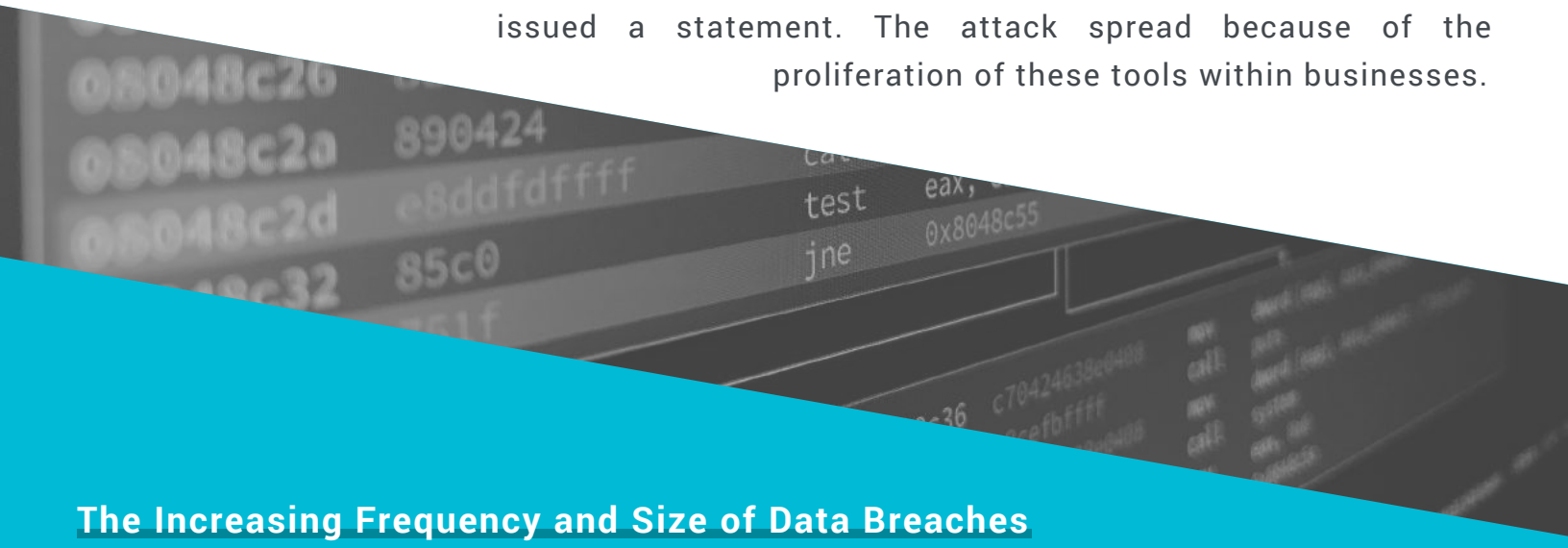
With companies of all sizes, from startup to enterprise, more frequently trusting cloud vendors in all aspects of their business, the market is flooded with new SaaS technology companies offering the 'next great product' to overhaul how people do business. With the

shift to cloud-only and the adoption of varying SaaS products and cloud infrastructures, companies are working with more and more third party vendors, opening themselves up to security risks that are out of their control and in the hands of their vendors.

In addition, SaaS products present the opportunity for seamless integration to other vendors. This is why one of the biggest concerns on the minds of security teams is understanding what internal systems and data new vendors have access to. In a recent survey, security was cited as one of the leading concerns of APIs and integrations. When it comes to these third party integrations, OAuth is the most widely accepted standard, "but there are still many APIs out there today relying on Basic Auth (17%), or some custom implementation of API Key & Secret (33%)."

Google

In many situations, your organization's employees think they're just adding a tool to their Google Apps account, and they don't understand how that simple activity can create monumental risk. They don't think about all of the other connected apps and implications that one integration can have on the security of the entire business. But no vendor is untouchable as even Google Docs experienced a recent phishing attack that was so severe the United States Computer Emergency Readiness Team issued a statement. The attack spread because of the proliferation of these tools within businesses.



The Increasing Frequency and Size of Data Breaches

What do these cyber security incidents look like and who do they affect? According to the Center for Internet Security, in 2015, there were 79,790 cyber security incidents (an incident is defined as any event that compromises the confidentiality, integrity or availability of an information asset), with 2,122 of these events confirming data loss. Unfortunately, small to midsize companies with fewer than 1,000 employees are bearing the brunt of these incidents, with Security Magazine reporting that 60% of these companies end up going out of business within 6 months after a breach.

THE INCREASING FREQUENCY AND SIZE OF DATA BREACHES

Breaches can take a major toll on a company's overall perception in the market, regardless of how large or small the organization.

CASE STUDY:

Take Yahoo, for example, which lost over $2 billion in market value overnight following the announcement of their massive data breach.

The Current Scope of Third Party Security Incidents

The issues that companies open themselves up to when doing business with hundreds or thousands of third party vendors at a time are significant, but tend to only come to light once an incident occurs. It is crucial that organizations understand the current landscape of third party security before an issue occurs, which could result in a loss of money, trust or personnel.

CASE STUDY:

A 2013 Trustwave study revealed that because so many businesses embrace an outsourced IT operations model like the one mentioned above, 63% of data breaches were in some way linked to a third party vendor.

Once hackers have gained access to a company's records via a third party vendor, there are multiple directions they can proceed. PWC reports that, in the case of the hacking of a midsize company, 31% of the time, hackers compromise employee records, and 27% of the time, they compromise customer records. Less frequently, hackers steal intellectual property or compromise partner or customer information, which incurs financial loss or interrupts business processes.

Why are Incidents Like This Taking Place?

Most organizations are not aware of who their third party vendors are, what they are doing, and how secure (or not secure) they are. In a report from the Ponemon Institute in March 2016, it was found that only 33% of companies have an inventory of their third party vendors and the data they have access to.

Ponemon institute also found that most companies are not able to confirm if third parties have recently seen a data breach or cyber attack or whether or not the third parties are sharing their confidential information and with whom they are sharing it. Finally, Ponemon found that companies are rarely, if ever, conducting reviews of vendor management policies in order to address data risk.

Cisco found that IT departments estimate that their companies are using an average of 51 cloud services, when, in reality, they are actually using an average of 730 cloud services.

This internal awareness gap of nearly 15X—a monumental disconnect by anyone's standards—demonstrates the idea of "Shadow IT", which is the grouping of cloud services that a company pays for and utilizes without involving IT (for example, cloud applications that employees pay for on a credit card).

In spite of all these findings, the Ponemon study reported that 73% of respondents see the number of cybersecurity incidents involving third party vendors increasing over time. So, why the disconnect?

Most companies in the Ponemon study cited "a lack of priority or resources" as the main cause for the current state of their third party security program. As we all know, priority and budget are not easy challenges to address. Regardless of the reasons for the deficiencies in third party security, however, there are some simple things that companies can begin doing today to raise awareness internally and improve the security of its third-party relationships, potentially garnering more resources and additional attention to this increasingly important part of information security.

Getting Your Leadership Team to Pay Attention to Third Party Security

While many executives are aware of the issues that can result from working with third party vendors, this doesn't always translate into additional resources or priorities for their Information Security teams. As your company works to protect its sensitive information while doing business with third party vendors, consider these five steps to raise internal awareness with your leadership team of the threats that third party vendors can pose.

1

Start building (or get access to) a list of all third party vendors

If the Information Security team doesn't currently have a complete list of all of your vendor relationships, this is where you should start. You should be able to, at any given time, review a complete list of all vendors along with a description of the product(s) or service(s) you are utilizing.

2

Document what sensitive data or internal applications all of your vendors have access to and use this to categorize each vendor by inherent risk

As you start building out the list of vendors, categorize the vendors by the type of data they touch or applications and systems they are connected to. Your organization may have done this already for your most critical vendors because of an audit requirement, but rarely do companies expand beyond that initial scope. You may be surprised by recently added tools that you weren't aware of, or by who has access to highly sensitive data, whether that is employee data, customer data, or any other data type you classify as risky or confidential.

3

Design an assessment process that matches the risk level of each vendor

There is nothing more frustrating to a vendor than a requirement to fill out a set of questions that have nothing to do with the services you are procuring from them. Customizing your security questions, documentation requests and recurring assessment cadence based on the vendor's risk-level will not only benefit the vendor, but will also prevent you from having to sift through information that is irrelevant due to unnecessary due diligence.

And don't forget to set a time frame to re-assess even your low-risk vendors. Security postures and product use-cases can change rapidly

and your organization can't afford to ignore hundreds of vendors under the assumption that they were reviewed once in the distant past.

4

Build an ongoing process to gather vendor information and data access as your company adds new vendors

Every time a new software is purchased, the security team should be involved in the procurement process. Meet with the procurement team or your business unit leadership to talk about how you can become aware of new purchases earlier on in the buying process. Communication is key and establishing a process to gather this information is helpful.

The employee purchasing the software typically has (or can easily get) the information you'll need in order to conduct an initial analysis of inherent risk and the level of assessment needed. This prevents the leaky-bucket syndrome where you can never catch up to the growing list of vendors that need assessments, regardless of how hard you try. And make sure you choose a central repository where you can store all of the security-related data from previous assessments and easily access it when it's time for the next assessment.

5

Select a few key leaders to meet with this month to get more buy-in across the organization

Your whole organization should be on board with the responsibility of protecting your company's sensitive information, but getting every single department engaged is a huge task for any security team. As a first step, select a few leaders and setup a meeting so you can start educating on what you are looking for in your security reviews, how to speed up the process of assessing a new vendor and the risks involved with third party vendors. This last piece (the "Why") is potentially the most important thing you can communicate with your team. The more they understand why you are asking them to pay more attention to information security, the more buy-in you can expect.

Is Your Organization Prepared?

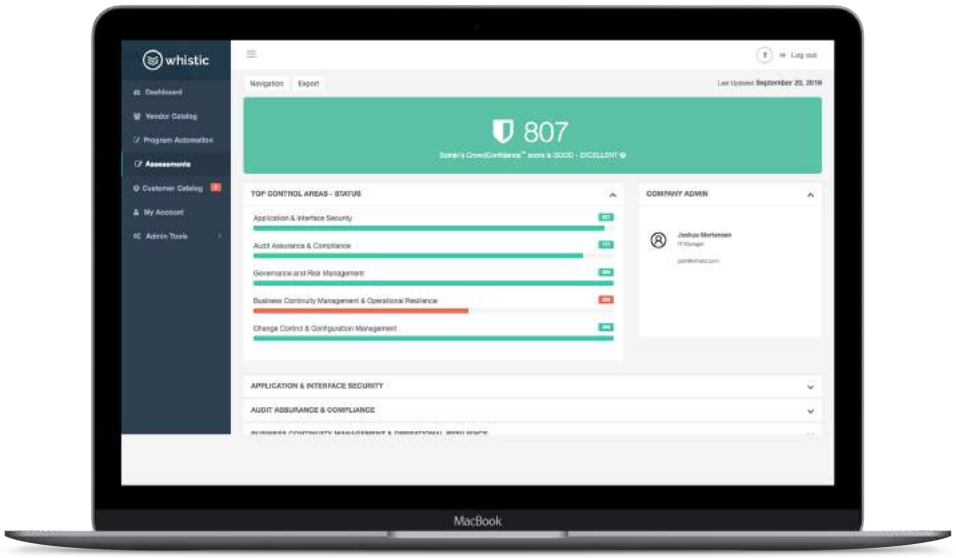
Effectively working with third party vendors should not be an unknown risk to your organization; nor should it be a detriment to the speed at which you do business. There are ways to manage security assessments that will ensure your Information Security team is always in the know. After taking an inventory of the ways in which your organization currently manages your third party vendors and reviewing how you can implement the suggestions proposed above, consider if Whistic could offer you some peace of mind in managing these risk assessments more effectively. After all, the more your organization understands what needs to happen to ensure security, the more they'll respect what you are doing.

Why wait to get started? Start taking the steps to protect your organization—and customers—today.

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 static security 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

CONTACT US

https://www.whistic.com

info@whistic.com

+1 800 655 6905

1982 W. Pleasant Grove Blvd. Suite H
Pleasant Grove, UT 84062