THRILLER

A TALE OF VENDOR RISK

What You Don't Know,
You Don't Know –
and It Can Be Catastrophic

SAI GLOBAL

The story before the story

Consider the story we're about to tell; a 21st-century CISO cyber-parable. The lesson here is that vendor risk management and third-party data breach prevention are essential if an enterprise is to survive.

InfoSec specialists and CISOs charged with ensuring data security for their companies probably never expected they'd have to wear so many hats: technical analyst and IT geek, detective and political traffic cop, faithful corporate warrior and organizational psychologist.

When bad news lands on their desk, the horse may have already left the barn, and happy endings aren't just a click or two away. In their world, data breaches go beyond the theoretical; for many, the fear isn't if, but when. The unknowns are how big and at what cost.

The urgency for proactive prevention is clear, but it isn't clear at all what that looks like.

And the risks get bigger as the bad guys get smarter: vendor risk management has never been so vital. What you don't know, you don't know – and that could mean exposure to an avoidable cyberattack that costs time and money, derails focus, damages your brand and your customers, and upends careers.

Yesterday's tools aren't enough to prevent or counteract third-party vendor breaches. Manual spreadsheets and obsolete, cobbled-together software can't defend against today's sophisticated attacks. Innocence doesn't absolve anyone of liability, and the consequences of liability can't be overstated.

Many CISOs build their careers the old-fashioned way. Smart, tough, and willing to pay their dues, chief information security officers earn their role through performance. Rewarded with a corner office, C-suite respect, and a seat at the big table, they wisely take none of it for granted. Success, while nice, is also precarious. Despite a bright future, CISOs generally have no illusions. They know that in today's digital Wild West lurk unseen, unknown enemies who are working just as hard as they are.

Now to our parable. Imagine that one of your key suppliers' data has been breached, an event that has made headlines. Your board, understandably alarmed, summons you to find out why they learned about it from media reports, along with the rest of the world, and not before.

The spreadsheet you use to manage vendors has no answers, but you have to find one.

Licking your wounds, you resolve to approach the challenges with a combat-ready mindset. Fueled by your professional pride, survival instinct, and acceptance that no one is immune to a threat, you commit to becoming an insatiable student of the current landscape.

First, you need to understand the problem and the potential consequences, then learn why others have failed to protect themselves. The goal: do everything in your power to prevent a data breach by identifying industry-leading solutions that are up to the challenges of today and tomorrow.

An epidemic of third-party vendor breaches

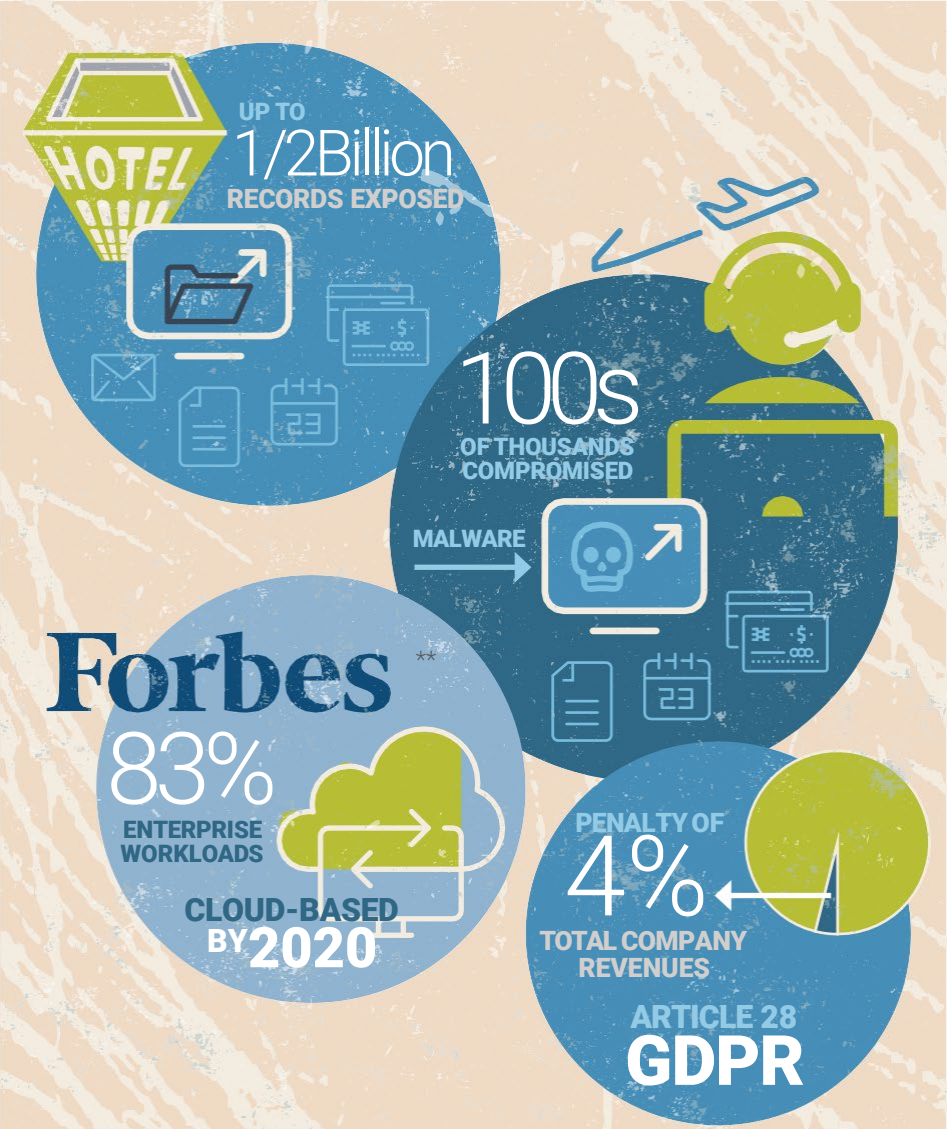
Any CISO worth their salt knows the price of failing to deliver on expectations. Another breach might be inevitable, but to ensure that you're adequately prepared next time, you call a meeting with your senior IT security managers to lay out the issues facing the company and enlist them in crafting a solution. You start by assigning each team member to research and report on third-party data breaches – say, one to gain an understanding of the overall trends, the scope of the problem, and which companies have been hit, and another to take on consequences and liability.

Your principal responsibility will be to study your current spreadsheet-based vendor management system to understand how it left you so exposed. Most important, though, you'll research solutions that give your company iron-clad security and that the board will be willing to support.

In just a few days of research, you learn some shocking facts. First, according to the November 2018 Ponemon Institute Study, 61% of data breaches are introduced via a third-party vendor*. One recent major breach cost the victim company $300 million – and counting. And it's not just customers, but core business services that are attacked. Another large-scale organization was hit when a remote access tool (RAT) was used to take control of a financial server.

Beyond the initial losses is the potential for a class-action lawsuit. Big companies often do business with hundreds, even thousands of vendors, and a company's defenses are only as good as those of the third parties it deals with.

You're now picturing the spreadsheet your company uses to track over 600 vendors – how little it tells you, how little it does, and how vulnerable the company is because the spreadsheet offers no protection but simply summarizes your company's considerable risk.



And there are more cautionary tales, the latest being the massive hack breach at hotel group Marriott International. Marriott said a hack that began four years ago exposed the records of up to half a billion guests in its Starwood Hotels reservation system. Guest addresses, emails, dates of birth, credit card numbers, and Starwood reservation information may have been stolen.

Further, a chat and customer service vendor for Delta Air Lines, Best Buy, Sears and Kmart was recently hacked via malware and compromised credit card information, addresses, and other personal data of hundreds of thousands of customers. The list goes on.

As you consider these real-world examples, you point out to your team that the global trend to outsource third-party services to the cloud will only make things worse. What makes real operational sense on one level also exposes companies even further.

Forbes has estimated that by 2020, 83% of enterprise workloads will be cloud-based**. Further, many companies are even using fourth parties, and there's no way to know what their preventive measures are – if they have any.

Next, you learn about consequences and liability, but this is a short report. There's no mystery here: Compliance is a growing global matter, and it's blind to borders. But what's really scary are the penalties for noncompliance.

HIPAA, GLBA, and Dodd-Frank are just the start. The General Data Protection Regulation (GDPR) means that anyone doing business within the European Union – compromising the data of even a single EU citizen – is in the penalty crosshairs. It doesn't matter if the data is handled in-house or by third-party providers. Article 28 of the GDPR imposes a penalty of 4% of total company revenues. Fines can reach into the billions.

Spreadsheets: Don't bring mittens to a boxing match

Your company isn't alone: Many large enterprises manage vendors using tools that once seemed efficient, like spreadsheets. But these tools just aren't equipped to deal with current reality. You've all known that spreadsheets offered false security when it came to vendor risk management and compliance, but the board has been resistant to change. Now, you have data that will make the argument for you.

You craft a case for addressing vendor risk management, directed at the board. Your report starts at "Ground Zero," the realities of spreadsheets:

- Hard to manage, inconsistent, and incomplete; offer no way to find or remedy errors
- No oversight, with a real risk of intentional errors increasing the potential for fraud
- Great for calculations, but without validation, in the end offering little, if any, actual value
- Leave the company exposed to financial losses, and legal and reputational damages

You address each point in turn: Spreadsheets are static, not dynamic; manual, not automatic. And they can't scale or adapt. In fact, doing the right thing is actually counterintuitive, because managing spreadsheets more rigorously only compound errors and accentuates limitations.

In the end, it's clear that spreadsheets burn resources but give little back. There's no central repository or intelligence for collecting and collating data, no trends revealed, and no actionable insight harvested. And analytics? Forget it. Your team is all too familiar with these limitations, and they know firsthand that the current system for managing hundreds of vendors not only consumes time but exacerbates rather than mitigates risk.

But as far as your case to the board is concerned, this is your secret weapon: Spreadsheets don't meet regulatory requirements, and they put the company in real jeopardy of noncompliance. That invites disaster.

You can now move forward with a proposal to replace spreadsheets with an integrated, automated capability to manage vendor risk, proactively mitigate exposure to third-party data breaches, and assure compliance.

Vendor Risk Management defense

Your requirements document will articulate the need and starts by defining what real vendor risk management would look like and what a system would actually do, top to bottom. You know that, in the end, vendor risk management defense capability has to mean not settling for merely good enough.

To engineer it from the inside, you think like a client. The nature of the threats and their consequences mandate that any system must be functional in the real world and have best-of-all-worlds capabilities.

You develop a list of must-haves, and when it's complete, it is formidable:

- The system must feature integrated risk management capability to address cybersecurity risks, policies, and regulations. It needs to be a true end-to-end solution mapping PCI-DSS, HIPAA, and all regulations so that the company can see the gaps between regulatory requirements and a vendor's actual performance. Flexibility for industry-accepted frameworks is a must because any solution that can't be tailored to individual needs isn't good enough.
- Security engineers must be enabled to create controls, and the solution must generate meaningful reports – i.e., they account for data automatically collected, stored, and analyzed. In the event of a third-party breach, these reports must go a long way toward satisfying the needs of stakeholders, including customers, insurers, investors, regulators, and management.
- Vendors should be subjected to an initial vendor risk baseline of low, medium, or high; performance would be measured with ongoing assessments that show patterns and changes. It would be a bonus if analytics databases and applied BI could be leveraged to graphically present real-time findings, making them easily understood across the enterprise.
- Questionnaires must be automated and ongoing, keeping information fresh and never static. Intuitive communication tools and dynamic conversations with IT vendors, perhaps using chatbots, would keep everyone ahead of the curve, rather than chasing it.

And you want independent monitoring – and grading – of vendors in real time. Your team needs a system that offers an algorithmic calculation of the likelihood of a breach and its potential severity, vendor by vendor, as each gets scored in real time. This would replace assumptions with actionable insight and tell your company who to do business with and who to avoid.

Next, you outline for the board the need for automation to remedy any breaches. That means visibility across all vendors from a central location, as well as the ability to instantly trigger remediation and address the risks of zero-day attacks and new security threats.

Real-time information about breaches at vendors would mean being alerted sooner, escalating the ability to confirm, respond faster, send an automated questionnaire, and gather information to guide next steps. Threat intelligence feeds would match the new data with previous questionnaires, and you explain that the ability to compare the two could make all the difference in your company's response.

Understanding the impact of a changing security threat landscape is the key to effectively defending against it, so the system you describe to the board must query vendors to prevent data leaks proactively. This is part of an ongoing assessment of new regulations, security controls, and all other measures to safeguard the integrity of the enterprise environment.

In short, the need you outline is an organic solution with strict adherence to best practices. You also recognize that your enterprise needs a solution that can grow and mature along with you, evolving as the company's needs change. Customization is also key.

And, of course, the ideal provider needs to be top-shelf, committed to innovation and committed to a continuing relationship with your company. You've seen it before, and you know that implementation can't end with "good luck" and a disappearing act. The deployment has to be right on every point, including thorough staff training, on-demand support, and systematic review to assess progress and achieve constant improvement.

VENDOR RISK MANAGEMENT CAPABILITY FROM SAI GLOBAL

The Big Reveal: Your list of must-haves and nice-to-haves is found in a world-class solution that empowers you to manage vendors through the complete risk lifecycle at SAI Global.

Learn more. Visit us at saiglobal.com or better yet, contact us for a freedemo.

[solutions] to advance confidently

*Data Risk in the Third-Party Ecosystem: Second Annual Study. Ponemon Institute, November 2018.

**Columbus, Louis. "83% Of Enterprise Workloads Will Be In The Cloud By 2020". Forbes, January 7, 2018. www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#1842c5fb6261. Date Accessed Dec 10, 2018.

SAI Global helps organizations proactively manage risk to create trust and achieve business excellence, growth, and sustainability. Our integrated risk management solutions are a combination of leading capabilities, services and advisory offerings that operate across the entire risk lifecycle allowing businesses to focus elsewhere. Together, these tools and knowledge enable clients to develop an integrated view of risk. To see our tools in action, request a free demo.

We have global reach with locations across Europe, the Middle East, Africa, the Americas, Asia and the Pacific.

For more information visit www.saiglobal.com/risk.

SAI GLOBAL