Sizing Up Risks for Third-parties & Vendors

Third parties and vendors can bring a lot of value to the table – but with that also comes risk. How do you assess, address, and mitigate?

SAI GLOBAL

Table of Contents

Executive Summary

With today's interconnected, interdependent nature of businesses and the emerging strategy of hacking into this web of relationships, the disruptive spectre of third-party risk continues to loom ever-larger. It's estimated that 65% of today's cyber breaches are caused by third parties. And while many organizations may have taken the cybersecurity of third parties for granted in the past, with many having had to get their house in order with the EU's General Data Protection Regulation (GDPR), the stakes for protecting your business from cyber threats have never been higher. There's simply no room for casual business relationships based on blind trust.

As a result of the escalating risk and fallout when third-party risk becomes reality, many organizations are continuing down the path towards adopting the right cybersecurity posture and implementing robust third-party risk management. By doing so and ensuring that it is applied to its entire network of partners, an organization can effectively manage and mitigate third-party risk. Without an effective risk management program an organization faces real and tangible damning impacts in the form of financial losses – the average global cost of a data breach stands at an estimated US$3.86 million – customer losses, and reputational and brand damage.

With breaches and security incidents affecting third-parties and vendors continuing to dominate the headlines, there's been an erosion of consumer trust in the commercial marketplace, specifically as it relates to data stewardship. According to respondents to SAI Global's 2019 Reputation Trust Index report, 59 percent say they are less likely to trust a company that has had a data breach. Across the board, 65 percent of those surveyed viewed data privacy as the most important attribute when considering a company's trustworthiness. With 75 percent saying they would accept a lower quality product for increased data protection. They would also pay more for a product or service if data privacy was guaranteed. This illustrates that data security is more than just a compliance issue, but one of trust and reputation.

In light of protecting yourself and your customers, more than ever you have a strong incentive to broaden and deepen the way you manage third-party and vendor relationships. It's not enough to ensure that your own house is in order – you have to assess every business relationship. After all, a chain is only as strong as its weakest link. And cybercriminals are adept at finding weak spots.

But sizing up vendor and third-party risk is a tricky business, which is why we have created this ebook to help you and your organization to assess, address and mitigate the risk of third parties and vendors.

Understanding Risks in a Roundabout Way

Instead of seeking to achieve the impossible and understand all risks a business faces, a better – or saner – approach is to look at the criticality of known, identifiable risks. Risk criticality involves looking 'around' the vendor. That is, assess the vendor's necessity in the first place by asking questions all around their purported need, instead of more direct questions. For example:

- What might the vendor's data access *frequency* be like? Would that be the same, or change over time? Or by some other measure (e.g., as new records are added/deleted)?
- What levels of data *sensitivity* does the vendor need? Can they clearly articulate which kinds, and why? Can they state what they will not need access to?
- Which *country or countries* does the vendor operate in, from a labor perspective? What about from an electronic data storage perspective?

This list isn't exhaustive, but rather illustrative to explain a different way to size up a vendor or third party. Responses to those questions should not only yield answers, but also a visceral reaction to how important or critical a misstep in that particular area could be to your business.

Using risk criticality as a yardstick

Here are ten risk areas you should consider probing when assessing the criticality of risks for any particular vendor. As you think about these areas and the suggested facets to probe, document how one area might be more important, or critical, than another. The key to this exercise isn't just understanding more about the risks, but to what degree they affect your business.

Core company risks:

FINANCIAL CRIMES AND SANCTIONS RISK

Are there protections in place to ensure your customers and suppliers aren't laundering money for nefarious purposes or financing terrorists? Know Your Customer (KYC) provisions demand you know who you're doing business with, even in less advanced countries where it's harder to know these answers.

FINANCIAL STABILITY

How financially sound is this vendor or third party? Are they profitable? Or, do they have money in the bank, sufficient to last the duration of your foreseeable partnership with them? If a potential partner hits financial bumps in the road, then that could cause them to focus on things other than your partnership – a potential upset for your customers.

LEGAL RISK

What is the partner's track record with past or pending lawsuits? Are they generally litigious? Similar to a potential financial situation, avoid a third party or vendor who has or will have to spend considerable time with lawyers and courtrooms, stealing time from forging a solid partnership with your business.

Instead of seeking to achieve the impossible and understand all risks a business faces, a better – or saner – approach is to look at the criticality of known, identifiable risks.

STRATEGIC RISK

Is this vendor partnering with others in the same space? Moreover, are they partnering with a competitor? Is there a chance that your proprietary knowledge could be leaked?

TECHNICAL STABILITY

Is the third party technically sound with respect to systems and infrastructure? Do they have documented uptime, and does it meet your minimum requirements? Do their multiple technical tools and services communicate correctly with one another?

Business-specific risk areas:

COMPLIANCE RISK

Does the vendor 'walk the talk' when it comes to ensuring that they operate by the book? Does this vendor comply with the numerous regulations and standards in their space? Moreover, do they comply with the standards in your space, if they are different?

PROJECT, OPERATIONAL, AND PERFORMANCE ADEQUACY

How well-staffed and resourced is the third party? Do they have adequate human labor to carry out the duration of the relationship? Do they have a contingency plan in the event of attrition or sickness? Are the people well-skilled? Are the people a core part of that business, or outsourced (thus representing a *fourth*-party relationship)?

Do they have adequate resources to carry out the work required to maintain your business relationship? Have they adequately scoped upstream and downstream dependencies? Do they have a deep view into their supply chain? Can the vendor deliver on time and on budget?

DATA PRIVACY RISK

How well-versed is the third party in terms of maintaining data privacy? Are they keenly aware of all the various global regulations and requirements, depending on the level of sensitivity of your customer data? Has the vendor put data privacy at risk in the past? Can they produce a response or reason for these transgressions? How often does the vendor review their own data privacy governance?

CORPORATE SOCIAL RESPONSIBILITY

Does the vendor operate in a socially conscious way? Do their external values align with your business's? Would partnering with a particular third-party result in your business appearing less socially responsible?

BRAND AND REPUTATION RISK

Can you assess what the customers' general perception is of the third-party's brand? How has the third party handled crisis in the past? How resilient are they when bouncing back from a crisis? Would partnering with them elevate the stature of your company? How likely is a crisis on their part going to negatively affect your business? How quickly could your business address and mitigate a crisis your vendor has, even if not related to your partnership?

Criticality Assessed – Now What?

You've stack-ranked many of the risks that third parties and vendors can introduce into your business. Now you need to determine how you can mitigate them, should you move forward. But how can a business mitigate these risks to make the introduction of a vendor more palpable? And what can you do in advance to plan for a potential misstep, so you stay resilient and bounce back from a potential crisis? If something negative happens with your vendor, your customers won't care if the issue is ultimately theirs or yours – they will assume it's yours. So, protecting your brand and reputation is paramount.

This would never happen to me

At times, organizations are reluctant to believe the myriad of data that describes how much, how often, and how devastating malfeasance can actually be. They often think they are immune to it, suggesting that it only happens to others. Rest un-assured, though, that every brand who has been breached or subject to third-party malfeasance said the same thing, likely just prior.

Using third parties and vendors is par for the course – it's what makes a business operate. In fact, *eSecurityPlanet* reported that *181 third-party vendors access the average company's network each week*. Further, two-thirds of the companies surveyed said they've already experienced a data breach that was either definitely or possibly linked to a third-party vendor.

It's not a matter of *if*. It's a matter of *when*.

What's a company to do?

To prevent yourself from being in the unenviable position of having to backpedal and respond to a breach, the first step is to reduce the chances of getting to that point. As mentioned earlier, it's often critical for businesses to partner with third parties and vendors to operate their business. Once the risks and criticality of those risks are assessed, businesses can now put into play a mitigation plan.

Third-party and vendor risk mitigation can take many forms:

REQUIRE THE VENDOR TO CHANGE THEIR PROCESS OR BUSINESS TO MEET YOUR NEEDS

Depending on the severity of the risk and the willingness of the vendor, this is often the best approach…but also not often the easiest.

ENSURE A LEVEL OF TRUST THROUGH DOCUMENTATION

Third-party validation through certifications, reviews, audits, and the like can instill a level of confidence in the business that the third-party is operating to a satisfactory level.

PROTECTING AGAINST MISSTEPS WITH LEGAL LANGUAGE

Defining and agreeing to specific (minimum, average, etc.) levels of performance can be achieved with service-level agreements (SLAs). Further, these can limit liability or define recourse in the event that something in the partnership runs afoul.

PERIODICALLY CHECK ON THE PERFORMANCE OF THE VENDOR

Whether remote or on-site, checking that the vendor is indeed honoring their terms of the contract through actual observations demonstrates the business's level of concern to potential risk issues. Further, these observations can be regular or irregular; announced or unannounced.

TERMINATE THE VENDOR/BUSINESS RELATIONSHIP COMPLETELY

This may not address missteps from the past but severing the working relationship can prevent may further risks from occurring.

At times, organizations are reluctant to believe the myriad of data that describes how much, how often, and how devastating malfeasance can actually be.

Business continuity is complex. All areas of the business are subject to potential threats, however understanding the order in which processes and functions need to be recovered to maintain operations is imperative.

In Case of Emergency, Break Glass

Changing climates, business processes and even our growing dependence on technology and third-party vendors means that there is an increased risk for a multitude of business disruptions. To ensure stability, a robust business continuity plan (BCP) is crucial. A thorough BCP plan ensures all critical functions will continue to operate at minimum levels – or be recovered quickly – in the face of an outage to safeguard the longevity of the organization.

Business continuity is complex. All areas of the business are subject to potential threats, however understanding the order in which processes and functions need to be recovered to maintain operations is imperative. For instance,

- Is it more important to keep your online or brick and mortar store open?
- Is internet access necessary to deliver your goods and services?
- If facilities are inaccessible, where will your employees report for work, and when?

Further complicating the development of a plan is the level of dependence upon third-party vendors. What goods and services do they provide to your organization and how important are they in regard to the continuance of your business? Do they have a BC plan in place, when was it last tested, and what were the results in regard to the SLAs you hold with them? Many businesses often overlook planning for the scenario when a critical partner has a service outage. Just as Business Continuity Management is used to plan for an outage, Vendor Continuity Management should be applied to ensure all scenarios are covered.

The Book of Risk is Never Closed

You've spent considerable time building a BC plan – from basic due diligence to ranking internal and external risk levels to figuring out how you'll address issues. But unfortunately, you're not done. Risk evolves over time. Some get bigger. Some compound one another. Some are replaced by newer and more impactful risks.

Smart businesses need to stay agile. As our dependency on external changing business processes, vendors and technology deepens, risks keep evolving as well. You simply can't rely on checking in once per year. Evaluating risks and the plans to mitigate them, to be continuous, robust, and improve over time. As the saying goes, "you need the right tool for the job." And in this case, the right tool, or tools, are ones that can help you respond and react to the ever-changing risks of the business landscape. The best tools, therefore, will not only aid in capturing the data, but also enable the business to query and report on that data, notify when important changes occur, and suggest actions for addressing, before issues get out of hand.

Assess, address and mitigate your third-party risks with a powerful solution that empowers you to efficiently manage vendors through the complete vendor risk lifecycle.

CONTACT US TO SEE A PERSONALIZED SOLUTION DEMO

About SAI Global

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**.