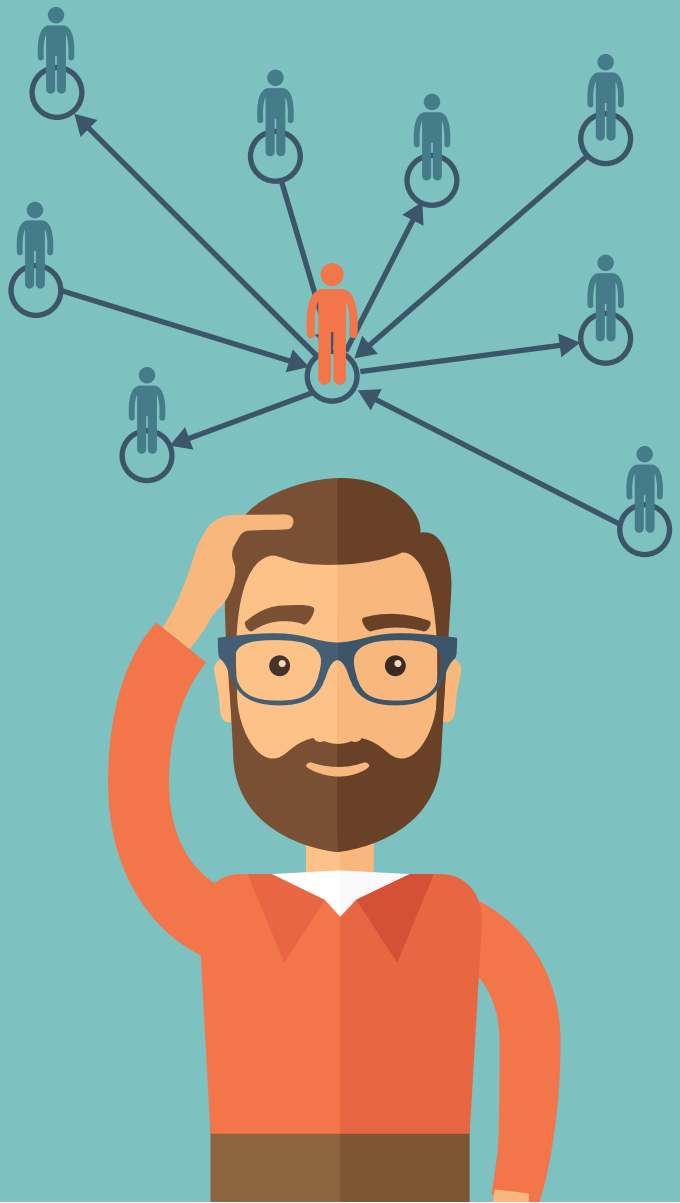
Vendor Risk Management

The Basic Need for It, and the Basic Principles of It

RECIPROCITY

rethink compliance.



Vendor Risk Management

As a concept, vendor risk is nothing new to most CISOs. The *urgency* of the problem, on the other hand—how quickly vendors proliferate, the range of risks they bring, the sheer number of vendors to manage— that has reached levels we've never before seen.

To put it another way, changes in technology and the business environment have expanded the risks that vendors pose to your organization, and expanded them dramatically. As a result, the need for *effective vendor risk management* has soared up the priority list for most CISOs. Depending on your industry and business processes, it may well be at the top.

This paper explores several dimensions of that challenge. First, why are vendor risks proliferating—why now, and where do they come from? Second, what steps are necessary to manage vendor risks? And third, how can CISOs and compliance officers implement those steps in a practical way, so you don't spend all your time chasing vendors with risk management protocols?

The Risk That Just Keeps Coming

Foremost, vendor risks are rising because companies are using more vendors in more ways.

A generation ago, companies typically would use vendors to buy goods (product components, computer equipment, furniture for the office); or occasional services (installing a new HVAC system, performing the annual financial audit, preparing the company for a merger). Vendors did pose risk, but those risks were discrete threats that existed only for specific periods. After the goods were delivered or services performed, the vendor went away. So did the risk.

The rise of cloud computing has erased that equation. Today companies use vendors for constant, ongoing services: data storage, human resources, payroll processing, financial reporting, customer relationship management. Rather than buy a software application, companies buy the service that a software application provides. The vendor never leaves your "extended enterprise." Therefore the risk never does, either.

According to a September 2017 study from the Ponemon Institute, which survey more than 600 senior executives, the average number of third parties with access to confidential or sensitive information jumped 25 percent last year, from 378 to 471. At large corporations, the number of vendors can easily run into the thousands. Other unsettling findings from the report:

- Only **17 percent** of respondents rated their oversight of third-party risk as highly effective;
- **57 percent** said they cannot determine whether vendors' safeguards and security policies are sufficient to prevent a data breach;
- More than half of respondents admitted they don't have a comprehensive inventory of all third parties with whom they share confidential or sensitive information.

Many companies are lucky if they even know how many vendors they have at all, because finding and using vendors has never been easier. In many instances, an employee (or even a third party working within your organization) can locate a vendor online and purchase services with little more than a company-issued payment card. Suddenly the business has one more vendor in its world, and one more vendor risk that poses a potential threat.

Why Vendors Pose Risk

So what risks do vendors pose, exactly? We can put them in several categories.

First, vendors can pose *regulatory* risks: whatever regulatory infraction they create while working for you, liability for that infraction passes along to your company as well. For example, if you store customer records with an outsourced data storage provider, and that provider experiences a breach—*your* business may be liable for damage your customers suffer, and your business is responsible for complying with any necessary breach disclosure laws. Or if that storage provider moves your customers' personal data across borders without the customers' consent, your business might be liable. (This will be all the more true starting in May 2018, when the European Union's General Data Protection Regulation goes into effect.)

Vendors can also pose *operational* risks: they cease working at critical moments and disrupt your business, or just not work as well as intended. While that threat can sometimes be alleviated with insurance policies for business interruption, in other circumstances an insurance payout is beside the point. For example, inefficient email or HR systems might tempt exasperated employees to seek new jobs. An HVAC vendor with weak security controls might be the side door hackers use to access your payment system and steal money.

Perhaps worst of all, vendors can pose *reputation* risks: their misconduct, somewhere down your supply chain, spills into public view and reflects poorly on your company's brand value. Nobody remembers the HVAC vendor that led to the breach of 41 million customer payment cards at Target in 2013. Everybody remembers Target.

This is the world that CISOs face: an increasing number of vendors, flitting in and out of your extended enterprise, often without you knowing; and an increasing number of risks those vendors bring to your organization—risks far more serious than anything vendors might have inflicted 30 years ago.

The Building Blocks of Vendor Risk Management

Vendor risk management happens in two phases. First, a CISO must evaluate prospective vendors *before* they graft onto your IT environment. Second, the security and compliance functions must then monitor vendors even after they become part of your extended enterprise, to confirm that their behavior— or possibly yours— has not changed in some way that has created new risk since their arrival.

Onboarding is the process of reviewing a vendor before allowing it into your IT environment. Your firm performs a certain amount of due diligence on the prospective vendor, to ensure it has sufficient controls and practices given the risks it might bring to your organization.

That due diligence can take many forms: a questionnaire submitted to the vendor, inquiring about its security controls and practices; attestations that the vendor has read your Code of Conduct and will follow it when handling your firm's data; outside audits, such as a SOC 2 Type II report to test the that the vendor has properly designed controls *and* those controls work as intended. Even simple reference checks or "adverse media reports" can count as due diligence.

The key to due diligence is that it should be risk-based; you undertake whatever steps seem necessary *given the vendor's potential risk to your organization.* For example, if your company collects personally identifiable information (PII) from customers in Europe, you will need to evaluate where, physically, a data storage vendor keeps those records—and its policies to ensure no vendor employees accidentally move that EU citizen data across borders. On the other hand, if your company does not collect PII at all, you might be able to exclude privacy controls from a SOC 2 audit since no PII is at risk.

The key to due diligence is that it should be risk-based; you undertake whatever steps seem necessary given the vendor's potential risk to your organization.

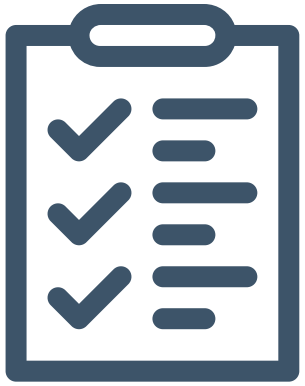
The Building Blocks of Vendor Risk Management (Continued)

CISOs need to ask:

- What data are we collecting and using?
- What risks do we have (regulatory, operational, reputational) in handling data that way?
- And therefore, what assurances do we need from vendors that they, too, can manage those risks while acting as part of our IT environment?

Once a prospective vendor passes those due diligence checks, **monitoring** is a crucial, ongoing task. Vendors may adopt new technologies or open new data centers. They might merge with other firms and change the terms of contracts. What's more, *your* business might change its operating model, and add new risks to the picture. Perhaps a sales manager starts collecting the names and birthdays of clients' children, and stores them in the cloud. Even if your data collection policies allow that, your vendors' data *protection* controls might not meet the heightened requirements necessary for PII of minors.

Again, the proper amount of monitoring depends on the risks the vendor poses. If you need access to a payroll processor system only 10 hours a week, a service-level agreement stipulating security and availability metrics might suffice. In contrast, mission-critical systems (anti-intrusion security systems to protect customers' financial data, for example) may need round the clock monitoring to ensure constant availability, as well as a requirement for an annual SOC 2 report to be provided.



The Inside Challenge

CISOs already understand the threat of "shadow IT," where employees bring new equipment, applications, or services into the company's IT environment without informing the IT department. The risk is real, but the name isn't quite right. A more accurate term would be shadow process— where employees can onboard vendors without the due diligence and monitoring steps outlined above. They have a process that exists outside yours.

That is the fundamental challenge for CISOs: to build a vendor risk management process that seals up any opportunity for others to bring vendors into your enterprise without proper oversight. It requires astute risk assessment, policy management, employee training, and oversight. It's a challenge that resides with the compliance department (which, after all, oversees policy management much of the time) as much as it resides with the CISO or IT department.

The fundamental challenge for CISOs is to build a vendor risk management process that seals up any opportunity for others to bring vendors into your enterprise without proper oversight.

Another challenge, of course, is convincing those employees in the operating units to respect the need for vendor risk management, and to see it as a benefit for the company. It most certainly is.

Strong vendor risk management means that the company has strong control over its processes generally—which, in turn, will give the company an easier path to compliance with the GDPR, New York's new cybersecurity regulations, industry specific regulations in banking or healthcare, and even SOX compliance for financial reporting. Achieving that high level of rigor also makes your own business a better, more trustworthy business partner.

In short, strong vendor risk management within your own operations not only reduces risk to you; *it makes you a more attractive vendor to other businesses.* Vendor risk management can be a crucial strategic advantage— which is good news, since vendor risk is likely to be one of the most vexing challenges CISOs face.

Steps to Take Now

1. Inventory the vendors you have.

You can't know the amount of vendor risk you have without knowing how many vendors you have in the first place. Start there. Count the number of vendors receiving checks from the accounts payable office; catalog the names of those businesses. Where possible, identify both the principal owners of each vendor and the persons within your enterprise who brought the vendor aboard.

2. Talk to your employees.

Spoiler alert: your vendor inventory is incomplete. No matter how thorough your accounts payable or procurement team may be, someone within the enterprise contracted with a vendor and didn't report that transaction. (Perhaps, for example, an employee put a vendor's charge on a company payment card and mis-categorized the transaction, so the accounting team doesn't know it's a vendor expense.) The CISO and compliance teams need to talk with employees about the threat of vendor risk, so they can understand the risk and help by raising concerns they know. They will know more than you.

3. Map your risks to assurance needs.

Put the vendors aside for a moment, to focus on the risks you face as an enterprise. How many regulatory risks do you have around privacy? How many operational concerns about security or business continuity? Then determine what levels of assurance you want that those risks are controlled to an appropriate degree. And then, after you know the assurance you will need, you can consider how to obtain that level of assurance from vendors participating in those business processes.

4. Consider the due diligence tools and monitoring processes you'll need.

Once you inventory your vendors, understand your risks, and know the assurance you want over them—you still have the actual work of managing vendors. That will require tools to perform due diligence before a prospective vendor is "onboarded," and processes to monitor them once aboard. The good news: much of that work can be automated. Still, CISOs and compliance officers will need to assemble the resources necessary to get the job done.