ClearOPS

WHAT IS VENDOR MONITORING? A GUIDE ON HOW TO MANAGE VENDORS.

For the better part of the last decade, I was the General Counsel at rapidly accelerating startups. I was also an early employee. This latter point is important because it means that I build processes from scratch. Not surprisingly, these startups did not have a vendor management process in place, so I built them.

Okay, so let me ask you. What are you doing for vendor management at your company? I know you can't really answer me (although I would love it if you did). But if your answer is "nothing" then this guide is for you. If your answer is "I have a long list of all the vendors we use and that's it" then this guide is for you. If your answer is "we only have about 3-4 vendors," then I don't think you understand what vendor management is.

If you are using software for your vendor management currently, well, then this guide is *not* for you. You seem to already be covered.

Let's begin with the basics. When I use the term "vendor" I mean a company providing your company (the "buyer") with services. It doesn't matter if that vendor is processing data or not and it certainly doesn't matter if the processing involves sensitive data or personally identifiable data. This is where many people make a mistake because they wrongly believe they can reduce the number of vendors they need to monitor by narrowly defining who qualifies (I am looking at you "I have only 3 vendors" responders). I have met many people who insist their only vendor is AWS, their cloud provider. Unfortunately, your threat landscape is much larger than that.

---

3 CRITICAL STEPS TO BUILD YOUR PROGRAM

If you recall the Target breach from many years ago, the vendor who caused that breach was a HVAC repair vendor. What type of data does a HVAC vendor process? I would presume only the data on how the air conditioning was working, but that was not they case. This HVAC vendor had access to Target's network so they could monitor the system at all times for maximum efficiency. Take that as an example of why narrowly defining who qualifies as a vendor is insufficient. Make your definition of who qualifies as a vendor broad. You reduce your workload through your risk classification and due diligence process, not by narrowly scoping which vendors make the list.

When I use the term "vendor management" I am referring to the process that you use to qualify your vendors according to their risk profile and then conduct due diligence accordingly. Article 30 of the GDPR, NY Shield Act, CCPA etc. are regulations that require

all buyers to perform reasonable security due diligence on their vendors. These requirements mean that if you don't have a process of vendor management in place, then you are violating the law.

These laws were put in place due to the causal link between a breach and the harm to the downstream consumer. Before regulation, a breached company essentially passed the cost of the breach to the consumer ("Hey, we lost your information. Good luck with that."). By establishing that the buyer is liable, companies can no longer shift the cost of a security lapse to the consumers ("Hey, someone accessed your data through our mistake. We will cover you with credit monitoring for the next year, on us.").

A recent example of a vendor hack is the SolarWinds breach. While there were many causes for that breach, no one can deny that thousands of customers were affected which lead to hundreds of thousands of consumers being affected. The breadth of this breach is still undetermined, but SolarWinds has already had to testify before Congress and suffered massive reputational harm. For the SolarWinds customers, who will likely be responsible to their breached consumers for notification and potential credit monitoring, their own vendor management process in assessing SolarWinds will also come under scrutiny, even if just internal. (Note: SolarWinds was a very sophisticated hack involving a patch to their Orion software and it is unlikely that even the due diligence process suggested below would have caught the breach.) (Second Note: You are not expected to catch your vendor's breach, but you are expected to ask questions and get answers. The process alone encourages proactive security, rather than reactive security.)

So, with tens, hundreds and potentially thousands of vendors to manage, I am suggesting the following steps to get started:

First, determine your company's risk categories. I recommend establishing 3 risk categories, low, medium and high. For example, public data like your website content contains low risk to anyone if it is breached since the data is intended to be exposed publicly, so your vendor who hosts and creates your website designs may be low risk (I am thinking of a site like Canva). Similarly, your catering company for a company event likely does not have any data other than the type of food you want to serve (just be careful of their wifi access). However, if your employees' social security numbers and salary data was breached, that would be very bad, meaning your payroll provider should be in your highest risk category. The middle category can be your in between risk, such as your sales prospecting data. Most likely you obtained the data from a public source, like Linkedin, and input it into a CRM. You would hate for that collection of data to be exposed for company competitive reasons, but such a breach would not cause significant harm to a consumer since it is already public.

ClearOPS

Second, build and organize your vendor list. To build the list, you need to ask accounts payable for all the vendors your company is paying. This list could include consultants, law firms, accountants, research organizations, etc., who are also vendors, so don't exclude them. In addition, you need to find the shadow IT, so all those vendors that store company data without charging your company in dollars. Most companies will have an almost embarrassingly large list of vendors. At ClearOPS, we arrived at nearly 40 vendors before we even launched our product.

Third, assign the level of due diligence required for each vendor according to each risk category. Below is a table of the risk categories and the required due diligence in each category that we suggest using at ClearOPS:

Risk 3 – Public	Risk 2 - Confidential	Risk 1 - Strictly Confidential
Data that may be disclosed to the public. Vendors who do not pose any risk if the data they have access to is exposed.	Information that is marked confidential or that is verbally disclosed as confidential or that is reasonably understood to be confidential. May be shared internally or under a non-disclosure agreement. Vendors who pose a medium risk if the data they process is exposed (i.e. some reputational harm, loss of some business)	Highly sensitive data that may only be accessed by a select group of individuals based on need to know. Vendors who pose a high risk if the data they process is exposed (i.e. reputational harm, loss of significant amount of business, financial risk to consumers).
• Vendor must have a publicly available privacy policy (updated within the last year). • ClearOPS vendor report	• Vendor must have a publicly available privacy policy (updated within the last year). • ClearOPS vendor report • SOC2 Audit	• Vendor must have a publicly available privacy policy (updated within the last year). • ClearOPS vendor report • SOC2 Audit

	certification summary (or similar) • If no SOC2 certification (or similar), security questionnaire (lite)	certification of at least 3 Trust Principles (or similar). Nationally recognized auditor. • Security Questionnaire (full) • Artifacts (proof of policies) • Upgraded security features for implementation or integration and access (such as 2 factor auth)

As you can see, the trick to streamlining vendor management is not to reduce the number of vendors you are monitoring (although that is a good thing to do if it means you actually aren't using the excluded vendors i.e. just cutting back on vendor reliance altogether) but to tier the amount of due diligence work required. The last thing I would do is conduct the level of due diligence required in my Risk 1 category on all 40 vendors because it is overkill and heavily resource-consuming a.k.a. a waste of time. But I also wouldn't skip doing due diligence on a vendor who is in the Risk 3 category.

BEST ADVICE – DON'T WAIT

As a task that is always set for "later," vendor management becomes increasingly daunting the longer you push it off because the list grows. Most businesses consistently add new vendors over time, without deprecating old vendors, especially if the buyer is hiring. According to our research, the average number of vendors used by a single employee is 8. That is a lot! Exponential growth of a company's vendors means your management of them can get unwieldy very quickly.

It's best to retain all this information in, yup, you guessed it, a vendor. At the bare minimum, use excel to create your list and some sort of file storage system, like Dropbox, to store the questionnaires and artifacts. There are many more sophisticated and useful tools out there right now that offer automation in sending out the questionnaires as well as alerts of vendor status changes. Privacy technology is a growing industry and I am sure more vendor management tools will come to market. As a short plug for ClearOPS,

ClearOPS

our system is tailored to the process I laid out above, with the added benefit of constant monitoring on your behalf through our diligence reports. The point is, if an employee leaves, you don't want all the due diligence work they did on your vendors to leave with them. The regulators won't be taking your word for it.

In conclusion, vendor management is mandatory, so don't delay. Set up your process now and make it a company-wide habit. You will thank me later.