TREXIN INSIGHT PAPER

December 15, 2020

SUPPLIER MANAGEMENT

The good, the bad, and the solutions.

Co-Written By:

Rebecca Rakoski, Esquire, Co-Founder and Managing Partner at XPAN Law Group, LLC.

Glenn Kapetansky, Chief Security Officer and Technology Capability Lead at Trexin Consulting

The journey to the cloud was well underway, with years ahead of it—and then a pandemic hit. Over a period of months, the value proposition for pay-as-you-go computing services (versus owning your own servers/software, as well as a big chunk of networking and staff) tilted strongly toward "let's do it, and let's do it quickly."

And then the implications hit. The cloud can be at least as fast, secure, compliant, and even cost effective as on-premise IT, but won't achieve any of those objectives if managed the same way. The authors' companies have collectively spent thousands of hours guiding and coaching enterprises back into compliance and cost effectiveness. Our desire here is to share some of this experience around the impact on (and strategic importance of) Supplier Management.

One definition of Supplier Management is "the process that ensures that value is received for the money that an organization spends with its suppliers." It is not surprising that traditional Supplier Management organization focuses on contracts that clearly specify costs for services provided, usually with strategically-defined service/compliance levels and penalties.

But the cloud's "as-a-Service" model does not provide service levels with penalties; rather, services are "best effort" with at most an outage penalty that is far less than the business value of the service disruption or breach. Supplier Management is a constant struggle for many organizations. With over 56% of data breaches caused by a vendor, it is something organizations need to pay attention to and, frankly, do better. After all, many companies will tell you that they have entire departments dedicated to Supplier Management. The accelerated drive to the cloud represents an opportunity for Supplier Management to adjust (and develop the necessary staff skills) for this more strategic role in enterprise Business Continuity. Supplier Management organizations can learn from (and require assistance from!) IT departments, which have a head start on learning to manage and leverage this different model. In many enterprises, IT has shifted from a supplier of technology to a multi-disciplinary provider of services.

This emphasis on compliance and breaches in Supplier Management is purposeful. Nearly every data breach (whether real or a "scare") in which the authors have been involved over the past couple years is because the client's vendor has been breached or potentially compromised. With large data breaches being linked to third-party vendors, and the required adjustments for managing cloud "as-a-Service," the heightened importance of managing qualified, compliant vendors can be leveraged to drive effective Supplier Management change.

THE CLASSICS

It is practically impossible to discuss vendor breaches and Supplier Management without discussing the classic example of two third-party data breaches; Target's 2014 payment card system was compromised via an HVAC vendor, and Equifax's 2017 data breach (one of the largest in history) linked to a known flaw in outside software it was using (the Apache Struts framework). Equifax also pointed the finger at a malicious download link on its website to yet another vendor. And these are just two of the more well known incidents. The fact of the matter is, companies are impacted daily by breaches involving third-party vendors, threatening the financial stability and reputation of companies across all sectors of every industry.

WHY ARE VENDORS A TARGET?

Nearly every aspect of a business involves the use of vendors; things such as financial software, document management, and data storage. In addition, with the creation of "smart devices," nearly every piece of software or device connects to the internet. According to Richard George, the former National Security Agency technical director of information, "Cybersecurity really is a supply chain problem." It is not surprising that vendors have become such an enormous target for hackers. After all, infiltrating a vendor network can act as one-stop-shopping for a nefarious actor. Consider that as organizations use more and more vendors, and watch those threats increase exponentially. The issue is further heightened, and becomes more costly, because of the significant struggles organizations face when dealing with third-party vendor risk management, or rather, the lack thereof.

THE REGULATORY WRINKLE

In addition to the increased attention vendors receive from hackers, there is another issue that organizations need to consider in vendor selection and management—regulatory compliance. For example, banks, insurance companies, and financial services firms operating in the State of New York, i.e. covered entities under New York Department of Financial Services Cybersecurity Regulation ("NYDFS"), are required to have written policies and procedures in place that ensure the covered entity vets their vendors' information security systems. 23 NYCRR 500 § 500.11 (p7). To be sure, the policies and procedures cannot be out-of-the-box. They are required to be based on the covered entities' own internal environment and provide structure around its risk assessment procedure, which includes the security requirements to vendors and due diligence procedures. In essence, this regulatory requirement also means that covered entities should also have contractual provisions that permit the organization to evaluate and audit the security practices of their vendors.

And NYDFS is not the only regulatory wrinkle. More broadly, there are laws like the European Union's General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act of 2018 ("CCPA") that also require organizations to conduct due diligence and have appropriate contract terms in place to monitor the services provided by third parties related to data processing activities. What is clear is that regulations are providing regulators (i.e. the individuals charged with enforcing these laws) more direct authority to require organizations to address third-party risks.

STOP THE INSANITY!

While Supplier Management and due diligence is clearly a persistent problem that every organization faces, it is not an insurmountable one. However, organizations keep doing the same thing over and over again, somehow believing that this time it will work. It seems obvious, but the definition of insanity is doing the same thing over and over again and expecting a different result. Stop the Insanity! The "trick" to Supplier Management is not to use or rely on a singular tech-only solution, but rather a multidisciplinary approach taken a step and a time.

The first thing that an organization can do is to rank their vendors in terms of criticality to the organization and data. In other words, the vendors that are essential to your business operations and the vendors that access the most sensitive information. This naturally means that you need to understand the data your organization collects and how it stores, shares, processes, etc., that data (i.e. a data categorization/data map).

Next, assemble the team that will be responsible for auditing the vendors. In order to take a multidisciplinary approach, you need a multidisciplinary team. The team should include legal and technical folks. Legal is there to ensure compliance with the contractual terms and regulatory obligations (what should be done), and the technical team counsels Legal on the capabilities/risks of the vendor systems (what can be done). By combining these two groups, you merge the two worlds in a constructive way. And the legal portion of the team can assist framing the issues in terms of obligations and liability that the technical portion alone cannot (and should not) do. Additionally, the team should not be an internal team. Vendors are always selected by the organization's departments. Using independent auditors creates more accountability and transparency. It also alleviates the issue of internal corporate politics that can influence vendor use and weaken the effectiveness of vendor auditing.

It is important to use time as one of your tools. In parallel (or even before) this team launches, implement the policy that all new vendor contracts contain an audit provision, specifying your right to audit, including by a third party of your choosing. Then, set yourself a pace that you can sustain for several years; select, say, your top five vendors each year in terms of criticality. If your contract already includes auditing, you need to notify the vendors that you are invoking your right to audit—otherwise, move down your criticality list until you have your set of five.

Send in your audit team to assess the vendor. The team should create both an internal report (written as attorney work-product) for your organization and an action plan for the vendor. Check up on your vendors periodically for status on the action plan, with escalation for poor progress. Then rinse and repeat, every year. After a few years, your vendors (even the ones further down the list and yet to be audited) will get the message and clean their own house, at least in terms of your account.

CONCLUSION

The Supplier Management conundrum is not a challenge that you can solve all at once, but you can start down the path before settling all the details. Here are some additional tips to consider:

- Realize that with the accelerating move to the cloud and Software-as-a-Service, vendors are increasingly strategic partners to your business operations.
- This represents a changed mindset for your Supplier Management organization, so partner with them to share your expertise as a team (Supplier Management, Legal, and IT).
- Create a roadmap, with a multi-year horizon—change takes time!

- This is one of those situations where it is smart to engage outside help; they have the expertise to coach your multi-disciplinary team on new behaviors, they preserve your own team's capacity to focus on their (now-changing) work, and they provide a valuable separation of perspective and duties.
- Consider the appropriate regulatory obligations (GDPR, CCPA, CPRA, NYDFS, etc.) for your business. Not only does it help focus your efforts on your specific obligations, but regulations are an important lever in ensuring cooperation from your vendors.
- Consider domestic frameworks and standards (NIST, CoBIT, ITILSM, PCI, SOC 2 Type 2, HIPAA/HITECH, etc.), choosing one that matches your regulatory obligations and is an appropriate "weight" for the size of your business.

It may take years to work your way through this process, but you will get there and remain compliant along the way!