The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No. 18 June 20, 2018

THIRD PARTIES

How to Maintain Effective and Secure Long-Term Vendor Relationships: Finding and Addressing the Issues (Part Two of Two)

By Amy Terry Sheehan, The Cybersecurity Law Report

For a vendor relationship to be long-lasting and effective, both sides should be able to identify when there are potential issues, communicate directly and address them in a timely manner. "Cyber thieves know that third parties often are a great one-stop shop for corporate clients' information," Karen Hornbeck, senior manager at Consilio, said during a recent webinar (recording available here) hosted by The Cybersecurity Law Report. Therefore, any mature data security program requires systematic and thorough oversight, clear leadership, the right tools to find gaps and efficient and appropriate action when issues are found.

See also "Developing an Effective Third-Party Management Program" (Mar. 14, 2018); and "How to Move Beyond a Checklist Approach to Third-Party Oversight" (Dec. 6, 2017).

Operational Best Practices

Being proactive and looking at the overall picture of third-party risk involves multiple departments and requires having a system that clearly sets forth who is coordinating the complex task of third-party oversight. The better the oversight process, the easier it will be to address issues as they arise.

"It's important to have operational systems in place" to ensure "gaps and issues are identified in the relationships, year in and year out," said Foley & Lardner partner Aaron Tantleff. While there are different ways of conducting vendor oversight, a company should have a group responsible for understanding all of its vendor contracts, whether that is a vendor outsourcing management group or a contract management group, he added.

See also "How to Effectively Find, Compensate and Structure Cybersecurity Leadership (Part One of Two)" (Dec. 14, 2016); Part Two (Jan. 11, 2017).

Form a Steering Committee

Hornbeck said she advises organizations to put a steering committee in place so that one group within the organization understands the high-risk information and is responsible for this overall effort within the organization. The group should include "everyone who has skin in the game."

Depending on how the business changes over time, there may be employee turnover, making it even more important to maintain a committee "made up of people who understand who your third parties are . . . and what the information is being shared."

The committee's standing members should include legal or compliance, risk, procurements and IT. "Legal or compliance will be able to offer insight into the regulations and the organization's obligations," Hornbeck said, noting that because there is so much regulation and litigation around third-party risk, it is becoming "more of a legal/compliance function."

Risk, procurement and IT groups have important roles as well. "Risk and procurement will bring the instruction and methodology for assessing who they do business with." IT "often has insight into some of the mechanisms and methodology by which information is shared," she added.

In addition to the standing members, "organizations should bring in people from the respective business areas who know the information that's being shared, as needed, depending on what the focus is at that time," Hornbeck explained, noting that they will know the risk and value of that information to the organization.

Use Audits to Stay Current

To help find any weak links and paint a complete picture of third-party risk, Hornbeck stressed the importance of periodic vendor cybersecurity and privacy audits and testing. This also makes for more informed vendor choices.

Companies should keep assessments and audits current with the changing threats and evolving landscape, advised Hornbeck, and "continue to reflect your business." Risk and data will change necessitating regular re-evaluation. This

should not be a "snapshot exercise"; it is something that organizations should execute on a regular basis, she said. For example, if an organization enters into mergers frequently and its subsidiary portfolio fluctuates, then its high-risk and high-value data will fluctuate as well.

Work With Technology Teams

Involving and engaging the information security and other technology teams on vendor oversight is crucial. "The info security teams and risk and compliance and privacy are obviously key partners," said Kristina Bergman, founder and CEO of Integris Software. Data infrastructure teams "control the pipeline [and] what technology is flowing in and out" – they are "best able to help provide you with the information around what kind of technology they use, what kinds of controls are in place [] and where the blind spots likely are." She added that they can work with the attorneys on creating a plan for mitigating that risk.

See "Tech Meets Legal Spotlight: Advice on Working With Information Security" (Jan. 11, 2017).

Bergan explained that the technical team will be able to add value to the process by informing on:

- how to mitigate risk from a technology standpoint;
- how to come up with technological approaches for vendor oversight;
- tools and technologies to meet business requirements on both sides of the vendor relationship; and
- vendor expectations that could potentially be written as contractual requirements.

See also our three-part series on when and how legal and information security should engage on cyber strategy: "It Starts With Governance" (Mar. 28, 2018); "Assessments and Incident Response" (Apr. 11, 2018); "Vendors and M&A" (Apr. 18, 2018).

Methods to Identify Specific Third-Party Issues

Hackers will find a weak link and it "may not be your direct vendor – it may somewhere else in the process, " Tantleff cautioned.

These steps are necessary because "cyber thieves are getting smarter and more efficient every day," Hornbeck said. While an organization "can assume that it knows how its third parties are securing your information, or it can ask," it should "never assume it knows the answer." Rather, the organization should "get clear, objective insight from everyone it is doing business with."

Ask Questions and Assign Scores

Hornbeck recommended that organizations seek a "set of key critical information to build a full-spectrum picture of vendors [they] are sharing critical information with" and have the information-gathering "driven by objective metrics" whereby each vendor achieves a score. She outlined the main categories that her team covers when seeking information from a third party for assessment:

1. About the Organization: What is the basic background information about the organization and its structure?
2. Geography: Where is the data stored/accessed globally? Where are the main offices? And, more importantly, where is the vendor potentially storing the company's information or from where is the information being accessed globally? Is there a major change in a third party data center that may impact your ability to access your own information?
3. Programs and Policies: Are they writing down policies regarding information security, data privacy, information retention and incident response policies and programs? And do they implement actual programs with people and funding around the policies to make them "actually operationalized throughout the organization?"
4. Privacy and Compliance: What do they understand about what privacy regulations and laws with which they're required to be compliant, either as a standalone entity or on your behalf?
5. Workforce Controls: What members of the workforce at their organization have access to your information? If it is everyone, ask why.
6. Infrastructure Security: How and where is client information hosted?
7. Application Security: How is data accessed and stored when utilizilng third-party hosted software applications?
8. Physical Security: How are certain rooms secure from a physical perspective? Is it clear where the organization's boundaries begin and end through proper signage and labeling?

9. Mobile and Remote Access: Is the usage of USB and/or portable storage devices allowed? If so, is encryption an option or requirement?
10. Storage, Recovery and Retention: Does the third party have an adequate backup and recovery plan? How long are they retaining your information once the contract ceases and the matter closes? Whenever possible, you want them to mirror your retention practices.
11. Monitoring and Incident Response: Do they have a monitoring and incident response policy? Do they have technology in place that not only detects intrusions, but also remotely disconnects those devices from the networks to isolate the problem as quickly as possible?
12. Third Parties: Are your third parties doing similar work with their own third parties because of the risk they inherited?
13. Cloud Services: Is the third party using cloud storage or software or any other cloud application? If yes, do they understand what cloud service due diligence and a cloud service contract should look like?

See also "Designing and Implementing a Three-Step Cybersecurity Framework for Assessing and Vetting Third Parties (Part One of Two)" (Apr. 8, 2015); Part Two (Apr. 22, 2015).

Use Technology

There are numerous ways in which technology can be used in third-party oversight and compliance, including by helping to meet the mapping requirement of Article 30; conducting spot checks; and finding specific records with a high degree of accuracy, Bergman said. "Manual-based processes give people a false sense of security and it's only with automated technology solutions that people can get an accurate measure of their risk," she suggested.

"I think the self-reporting and manual reporting that most organizations do is inaccurate, not out of malice, but out of lack of information," opined Bergman, and the lack of information "creates a false sense of security with companies that are managing third parties." Bergman said because data is changing with such "scale, volume, and velocity," organizations need a technical solution to validate what data vendors have and what it is being used for. "Manual surveys are not enough," she added.

In addition to using technology tools to gain information about third parties, organizations can use technology internally to prevent third-party issues. They can analyze streams of data leaving the organization to prevent oversharing of information that is not required (or permitted) under the contract and flag and issues, Bergman said. She suggested looking at newer technology that can handle both data in motion as well as data at rest, structured or unstructured, "regardless of where it sits, whether it's on premise or in a cloud data store."

Bergman also urged companies not to be shy about asking for what is technologically possible. Companies can expect vendors to do a lot with technology, Bergman said, including:

- identify what data in the third party's system has come from the organization and confirm whether it is still there (confirming application of retention policies) through AI tools;
- conduct spot audits on the actual data;
- provide the organization with the ability to view the company's data in its environment, whether through a web portal or self-service report;
- locate a specific individual's data within the organization;
- provide an audit trail for complying with data subject requests and data subjects' right to be forgotten; and
- provide proof of compliance with regulations like GDPR or PCI and compliance with contractual obligations.

There are limits to what technology can do and some tasks require human intervention. For example, technology can't interrogate third-party data centers, Bergman noted, stating, "There will always be things that can't be auto-discovered, like physical location and data centers, or the business purpose assigned to a particular use." Using just a manual or automated approach alone will not allow the company to "get a full picture." When both approaches are used together, "technology can marry the manual with the automated to make it very rich."

See also our three-part series on forensic firms: "Understanding and Leveraging Their Expertise From the Start" (Feb. 22, 2017); "Key Contract Considerations and Terms" (Mar. 8, 2017); and "Effective Vetting and Collaboration" (Mar. 22, 2017).

How to Address the Issues Once Identified

Whether it is through manual methods or cutting-edge technology, once issues or gaps are identified, they need to be addressed. Some organizations are hesitant to broach these topics, but experts advise they must.

Be Wary of Unwelcomed Feedback

"It's 2018. None of these conversations should be a surprise to any third party," suggested Hornbeck. "There is absolutely nothing wrong with having a conversation and getting all of [the issues] out on the table [by] reiterating how much you enjoy the working relationship," she opined, adding that it is then appropriate to state the company's expectations about how the third party is managing and securing the company's information.

The vast majority of third parties Hornbeck works with "welcome the feedback on their organization's assessment." If the third party "doesn't welcome the feedback, this should raise a red flag. If it pushes back and says that your expectations are unreasonable, that they don't make any sense, that they're cost-prohibitive, I think that that's really worth a deeper dive to the relationship as a whole, quite frankly, because everything that we always require or even recommend is based on industry standards" such as ISO, NIST, GDPR. "We're asking them to put very seasoned, sound best practices into place."

Set Priorities Based on Risk

Hornbeck recommends organizations take a risk-based approach whereby they have conversations with their vendors of all types and assess the level of risk "based on the type of information being shared," she said. Such an approach will allow the vendor "to focus on putting the most critical controls or policies or programs into place first," as opposed to just doing what might be easiest.

"If you know that you have a lot of high-risk information going over to someone that doesn't do very well on the assessment or audit. . . go back with a series of both requirements and recommendations," she advised. The vendor should be made to understand that, based on the nature of the information and how critical it is for the organization, "these are the things that [it will need] to put into place."

Negotiation Tips

There are different scenarios that may impact the negotiation approach with a third-party vendor. Companies may have certain requirements based on the GDPR, security obligations, changes in law or a change in the nature of the relationship," Tantleff said, adding that they also can sometimes point to an external force because in certain circumstances, "the obligations are either codified" or may stem from litigation. Tantleff often tries to start a conversation by stating: "This is not about renegotiating the agreement. This is about ensuring that both parties have proper language and proper protections in place to protect information because it's for both parties' advantage to ensure that those are there because both parties will have responsibility and liability and events if something goes awry."

"There are times you need to reopen the contract, " Tantleff said, and there are also times to end the relationship. If a company's vendors have security issues and they "aren't agreeing to even that which is reasonable and appropriate, it's time to walk away."

"That option of walking away has to be on the table," he said. "If you do the diligence and then still walk into it [or stay in the relationship] without proper protections in place, it invalidates [the process]. Regulators will not be thrilled with that. No one is thrilled with that because it makes the environment weak," he added.