The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No. 17 June 20, 2018

THIRD PARTIES

How to Maintain Effective and Secure Long-Term Vendor Relationships: Understanding the Risks (Part One of Two)

By Amy Terry Sheehan, The Cybersecurity Law Report

Once the critical process of vetting and selecting vendors is complete, the third-party oversight work begins. Change is inevitable – regulations, data sets, technology, products, circumstances – and organizations need to ensure that the vendor relationships keep up. "Parties need to work together well past when the contract is signed and put away," Aaron Tantleff, a Foley & Lardner partner, explained during a webinar (recording available here) hosted by The Cybersecurity Law Report. Well-managed relationships result in increased satisfaction, reduced costs and higher-quality service from the vendor. They can also serve to resolve any problems that arise more quickly, he said.

"In 2018, no vendor in the world should be put off by having conversations around how they're managing their clients' information," Karen Hornbeck, senior manager at Consilio, explained. Organizations "need to be making a risk-based assessment" to measure third party risk. This "helps drive the overall business decision."

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).

Regulatory Expectations

There are a wide range of regulations and laws that govern third-party relationships including the New York Department of Financial Services Cybersecurity Regulation, state data breach notification laws, the GDPR and other international laws such as those in Asia and Latin America, Tantleff said.

U.S. Regulators

Domestic regulators include the FTC, SEC and DOJ, Tantleff noted. Companies can meet regulatory expectations by following some simple rules – "apply an appropriate level of protection to the data that you have, properly secure it, don't misuse it and don't take advantage of people," he said.

Tantleff explained that the regulators are all looking to see that the organization has:

- conducted a risk analysis to determine how to secure the environment;
- applied the appropriate protections to the data (beyond just PI) and the system;
- properly notified the authorities and affected individuals following an incident;
- conducted proper investigation to determine what happened;
- implemented appropriate remediation to mitigate the impact; and
- put measures in place (i.e., proper training) to prevent a similar incident from happening again and/or expanding beyond the preceding incident.

These principles apply to handling of third-party relationships as well.

See also "Lessons and Trends From FTC's 2017 Privacy and Data Security Update: Enforcement Actions (Part One of Two)" (Jan. 31, 2018); Part Two (Feb. 14, 2018).

International Regulation

The E.U. has been an area of focus this year because of the significant changes the General Data Protection Regulation has brought, including new requirements for third-party oversight. However, other international data security regulations should not be ignored. Organizations collecting or sending data to third parties in jurisdictions outside of the E.U. must also ensure they understand and comply with a wide range of specific regulations.

GDPR

GDPR has the "most onerous" third-party oversight requirement "at the moment." It contains an "affirmative obligation to ensure that you have properly [conducted] diligence and that you have contractual protections in place to ensure the privacy and security of [personal] data," Tantleff said.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No. 17 June 20, 2018

Article 28 of the GDPR has "express provisions" about requirements for third parties that process personal data, including that they can only process that data "in accordance written instructions . . .[that] you have with your data subject" and "for nothing else," explained Tantleff. He also noted other requirements for third parties processing personal data, which include:

- acting only on documented instructions from the controller;
- notifying the controller regarding instructions that conflict with the GDPR;
- deleting or returning personal data at the direction of the controller upon request or at the end of processing (the third-party processor may only store data if permitted by applicable E.U. law);
- assisting controller in responding to requests from data subjects; and
- assisting controller in responding to requests from regulatory authorities and making required information available to the controller for compliance.

Under the GDPR, both the controller and processor are liable, Tantleff said. "A controller really needs to be very strong about ensuring that those contractual protections are there and not letting a processor [] try and do a light version of a contract" because supervisors could hold controllers liable for not having contractual protection in place "even if the processor is in compliance with the law," he added.

See also "The GDPR's Data Subject Rights and Why They Matter" (Feb. 28, 2018).

Other International Regulations

While the GDPR is obviously a focus, Tantleff advised that organizations should not forget about other countries, especially as there are "some other [regulations] that are actually more painful depending on what you are doing." The applicability of these regulations is not just based on jurisdiction, but also on the type of data the company is keeping, such as financial data, health care data, or data related to national security. "All these types of data, depending on what region you're in, will have different types of localization rules," he explained.

It is particularly important to focus on what laws apply when an organization is conducting "an onward transfer of data outside the borders of the country in which that data originates," Tantleff explained. For example, if an organization is transferring data from the E.U. to the U.S., it must meet the requirements of the Privacy Shield by (1) self-certifying with the U.S. Commerce Department; (2) attesting compliance with the Privacy Shield's principles; and (3) ensuring contracts with any third parties comply with the Privacy Shield's onward transfer requirements, Tantleff explained.

See also "Navigating the Early Months of Privacy Shield Certification Amidst Uncertainty" (Nov. 2, 2016).

In addition, there are different types of encryption and other similar laws in different countries. In certain countries, like Russia and China, "you have to hand over encryption keys to the government," and this could impact the validity of a safe-harbor type designation, Tantleff said.

See also "Guidance and Clarification on Asia's Evolving Cybersecurity and Data Protection Laws" (Apr. 18, 2018).

Understanding Legal and Compliance Risks

To stay ahead of the risk, organizations should "be proactive about having these conversations, setting expectations with the third party in terms of what to expect," both because it is good business practice and because certain things may be required for an organization to be compliant," Kristina Bergman, founder and CEO of Integris Software, explained, noting that compliance requirements include "vendors they share information with."

When it comes to identifying legal and compliance risks, "you can't just do your diligence when the contract is signed, you also have to do diligence throughout the process. Generally, on an annual basis, you need to audit the vendor, audit the process, ensure that third parties are adhering to the contract and then [evaluate] whether you need to change the actual provisions or change the obligation to keep up with current technology [or the] current threat environment," Tantleff explained.

Third-party legal and compliance risks can take many forms, including:

- vendor network access;
- contractual relationships;
- M&A;
- joint ventures;
- breach notification process;
- cross-border transfers;
- sub-processors; and
- data retention.

It is important to identify the risk category for each vendor. The process of evaluating risks starts with understanding "what information and what access" different third-party vendors have, Tantleff said. "Not everyone has the same level of risk. Obviously, third parties who have access to the system and have access to certain types of data will have an increased risk," and "that risk analysis will lead the charge in terms of the obligations that you're going to pose on those third parties."

This analysis and limiting the risk can be accomplished using security and privacy risk assessments, audit and oversight of third parties with access to data and/or networks and appropriate contractual protections, Tantleff added.

Contractual Provisions

Organizations need to make sure contractual provisions map onto legal requirements. For example, certain laws, such as the GDPR, "require that you have the ability to audit your processes" while some vendors refuse, stating they will "never agree to an audit" and will just produce a report, Tantleff said. It is important to understand how to address situations where a "vendor or processor says, 'I'm not going to provide you access but you're required" to have that access, he added.

Even if there is not an audit requirement, regular oversight is necessary. Many laws require regular vendor review based on changes in the environment, but may use different terminology in the legal requirement, Tantleff explained.

Data Retention

Organizations should make sure vendors do not hold on to data they do not need because that increases risk and can cause compliance issues. The GDPR states that companies may only hold on to data so long as they need it to process it or to accomplish the purpose for which it was provided, Tantleff pointed out. The data must be deleted or destroyed when the relevant tasks are complete or when the data subject requests it. Thus, a contract stating the vendor will hold onto data (even if it says it will keep it confidential) is not GDPR compliant, he added.

Collaboration and Communication

Organizations need to ensure the third parties provide "sufficient information" to meet their compliance obligations. They should also make sure "third parties are contractually obligated to assist them with anything that may need to be done . . . whether it is data impact assessment, audits, data access requests," or other compliance measures, some of which are required under certain laws such as GDPR, Tantleff explained.

In the event a vendor is "aware of any type of incident," it should be required to make the organization aware because the organization will have "affirmative obligations to make others aware," noted Tantleff. Notification periods vary by law, so the obligations need to be reviewed on a regular basis.

Subcontractors

Organizations should ensure that any contractual obligations placed on the vendor are contractually passed on to downstream subcontractors.

The GDPR, for example, states that subcontractors have the same obligations as the original contracting party, "although there's a lot of subjective interpretation," of that GDPR requirement, Tantleff said.

Understanding Technical Risks

In addition to legal and compliance risks, there are technical risks from ongoing third-party relationships that are not properly managed. The security risks of a vendor's network access have been well-publicized through the Target breach and others. In addition to those significant risks, there are lesser-known (but critical) risks around sharing data with third-party vendors, as well as accepting data from them.

Bergman noted that one of the biggest sources of risk is that companies are falsely confident that they know where their data is located and that they are able to effectively comply with relevant regulations, particularly in the event of a breach.

Monitoring Contractual Obligations

A disconnect between the contractual requirements and the on-the ground data practices can cause problems. There is often significantly "more data flowing from one organization to the next than what a contract stipulates," Bergman explained. For example, a vendor contract may state the vendor is not permitted to store location data for more than two years, but the "person setting up the data feed that's going out of your organization and into a third party might not be looking at the contract" and may not know what restrictions to set.

Data Lakes

Companies should recognize that data often flows into common repositories with very little delineation. "When companies share data, there's typically a misconception that that data is kept in isolation from everything else when in reality, it's not because that's not how infrastructures are architected," Bergman explained. This creates a risk because it creates more access to that data, she added.

Flowing and Moving Data

For the past 30 years, for "solid business reasons" such as availability, creating backups and geographic redundancy to prevent data loss, "data management best practices have been to make data flow like water through an organization," Bergman said. One company that Bergman works with was able to track a single transaction that was replicated 100 times throughout their system using that principle.

In addition, companies combine data sets and create derivative behavioral data that add values. But replicating and combining make data mapping extremely difficult, noted Bergman.

"Part of the challenge people face in managing third-party vendor relationships is that when they share data, they think it's a snapshot – it's a point in time and a defined group," Bergman explained. In fact, it is more likely a "constant stream" with "a pipeline of data leaving their organization and a pipe getting sucked into the other organization." The composition of data will shift and change. This misconception of a snapshot leads to "organizations miscalculating their risk," she added.

Locating Data

"From a technology standpoint, one of the biggest challenges that companies face is that they have no idea what data is where, they don't know where personal information exists," Bergman said.

For example, the CSO of a retail company with whom Bergman works makes a note if surveys for the company's survey-based data mapping come back the same every time. "He knows people are copying and pasting answers over." The CSO is "concerned that it's giving them a false sense of security about what data is sitting where because they don't actually have any idea of what's in their repositories. "When you're dealing with terabytes and petabytes of data, it's way too much information for anybody to actually go through on a manual basis." This lack of knowledge can make legal compliance difficult. "One of the biggest challenges with GDPR compliance is that most companies don't know what data is where and to exacerbate it, they don't even know what data is flowing into their organization, let alone what data is flowing out," Bergman said.

Newer, Less Secure Technology

While having "data flow like water" and the general movement toward a streaming architecture offers certain advantages and is considered a best practice, it also often introduces risk organizations may not be aware of. Only new types of technology can handle streaming data flowing through pipes and constantly moving, Bergman explained. When data lands in a "data lake" that could "include hundreds of terabytes, if not petabytes, of data," organizations should be aware that it will have less stringent controls on it because it will be handled with newer, less mature technology. "Newer technology, particularly anything used to process IoT data for streaming, is less mature technology and because of that, there are fewer security measures," she added.

Acquired Data

In some circumstances, due to acquisitions, for example, there are pipes with data flowing in and out of an organization that it might not keep track of. In those instances, the contracts that organization has with third parties will be "completely disconnected from the data," Bergman explained.

In joint ventures or M&A transactions or when companies share data with each other, the "technical risk" is that "most people just don't know the amount of data that's flowing" and "don't know what's in there," Bergman further emphasized.