Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Ensuring Vendors Aren't The Weak Link In Your Security Chain

Law360, New York (July 21, 2016, 11:31 AM ET) --


David Winters


Andrew Foreman

You've heard it a million times by now. Data breaches are happening all of the time. It's not a question of "if" your company will suffer a breach, but when.[1] And when it happens, it can be very bad.[2]

By now, everyone knows about the threat of a data breach and the need to do something about it. If your business handles or maintains the personally identifiable information of third parties or other regulated information, your organization may have to understand and comply with, at a minimum, the requirements imposed by data breach notification statutes in 47 different states. If your organization is a law firm, you have additional ethical obligations, including obligations of competency and confidentiality, which means you have to make reasonable efforts to protect your clients' confidential information. And there are numerous legal obligations that may apply to certain entities in specific lines of business, such as the Health Insurance Portability and Accountability Act[3], which regulates protected health information, and Gramm-Leach-Bliley[4], which regulates PII in the financial services industry. On top of all of this, your contractual counterparties may have imposed additional information security requirements on your organization. Plus, you know that good information security practices are good business — it's the right thing to do and it helps build and protect your brand.

On the other hand, your concern about information security means you've taken steps to ensure your organization is doing the right thing — well, you are reading an article on information security for vendors, so we're going to assume that's a safe bet. This means you've probably designated someone as the "security official," responsible for keeping regulated information, such as PHI and PII, as secure as possible. You're also forcing every person in your organization to change their passwords every three to six months, and you've made them choose a password other than "12345" or the name of your organization in all caps. So you are doing what you're supposed to do, or at least you're working on it, even if no one in your organization appreciates it. We understand how it works.

But it's not enough to get your own house in order. You have vendors. And your vendors are part of your organization's work processes and data flows. Worse still, you know that vendors are involved in a great many data breaches.[5] And you are responsible for making your work processes secure — and you may also be responsible in the event that a vendor is the weak link in the data flow.

So you have to think about the company that does your copying — and the company that cleans your

offices and empties your trash — and the information technology company that has access to your firm's entire network. The list may seem endless, but you've thought about it and you know that your vendors should be handling privileged and confidential information with the same care that you do.

It gives you a headache because in order to protect your organization's information, you've already attended countless trainings and spent hours in meetings trying to convince people in your organization to pay attention to these issues. Yet now you realize that you've got more work to do.

We're like you. So we've tried to provide a conceptual road map to help you think about information security and vendors.

OK, OK. I get it. What do I have to do?

First of all, get rid of the notions that your vendors will take care of their own security and that you do not need to worry about what they do. Reconceptualize the way you look at the role that vendors play. When it comes to vendors, you're assessing the risk of a "business process of which a vendor happens to be a part" — that's how R. Jason Straight of UnitedLex Corp. puts it (we're paraphrasing a bit). Straight's way of rethinking the role of vendors when assessing cybersecurity risk is powerful. The conceptual approach for managing vendors should mirror the conceptual approach for managing information security risk internally.

The approach with respect to vendors boils down to three basic elements that mirror the steps you have to take with respect to your organization's internal information security.

1. Do your homework about the vendor — your due diligence — just as you do with respect to your own employees.

2. Make a plan to manage risk. With vendors, this often starts with the contract.

3. Check in on your vendors to make sure they are doing what they're required to do. This is the place where a lot of well-conceived plans go astray.

At all points in the process, apply the concept of "risk stratification." "Risk stratification," or "stratification" for short, means that your organization applies different levels of risk management rigor based on the level of risk associated with a given vendor. For example, you may apply relatively modest requirements on the company that services the coffee machines and a far more rigorous level of risk management to a vendor that has access to your company's information network.[6]

1. Do Your Homework: Due Diligence

Due diligence with respect to vendors is nothing new, so most organizations will just have to add a step for assessing vendor information security — or enhance an existing procedure — to your due diligence process. Here are some factors to consider in assessing vendor information security.

Reputation

What is the vendor's reputation in general? Does the vendor have a good reputation in terms of information security? Has the vendor suffered some form of data or information breach in the past? That a vendor has suffered a data breach should not necessarily be a deal breaker — in fact, it may be a

deal maker. Vendors who have suffered data breaches and survived understand the costs of data breaches and may be more sophisticated than their competitors in managing risk. When you learn that a potential vendor has suffered a breach, ask: What happened? How did the company respond to the breach? And what did the company do to improve its processes and reduce the risk of future breaches?

Financial Condition and Insurance

A vendor's financial condition is an important factor to consider for reasons that go beyond information security; nobody wants their vendors to go broke. With respect to information security, you need to ensure that the vendor has the financial wherewithal to fund appropriate electronic and physical security.

If your organization has a cyber insurance policy — and most organizations should — you may wish to require that your vendors do as well, particularly if those vendors will have access to your organization's confidential information. While it may be sufficient to have some vendors warrant that they have a cyberinsurance policy and to explain the limits and scope of that policy, vendors with access to PII or PHI that your company maintains or uses should make their cyber insurance policy available for review.

Information Security Controls, Including Business Continuity

What are the vendor's information security policies, procedures and controls? Remember the principle of stratification. For certain vendors, asking them to certify that they have appropriate information security controls may be sufficient. But for vendors handling confidential information, you will want to review the vendor's controls and procedures and ensure that they comply with applicable law and your organization's standards.

Pay particular attention to the "point of transfer" of information between your organization and your potential vendors. If you're exchanging information electronically, does the vendor have appropriate controls on its end of the transaction to ensure that the transfer is secure? These controls should include procedures for properly disposing of confidential information after it is no longer needed or the relationship has ended.

Vendor Incident Response Plan

For vendors that will have access to confidential information, you should require that the vendor have in place an incident response plan. Depending on the amount of information to which the vendor has access, you may also wish to review the vendor's incident response plan and ask to what extent the vendor has had to use the plan. You may even want run "tabletop exercises"[7] to ensure that the plan works effectively and efficiently.

Employee Training and Awareness

It is not enough to have policies, procedures and controls in place. The vendors' employees must know about them. You should determine whether vendors have a robust program in place to train their employees. Again keeping in mind the principle of stratification, for some vendors, it may be enough to have the vendor certify that they have appropriate training and awareness protocols in place. For vendors that have access to your firm's PII and PHI, you will want to ask for more information, such as copies of any training materials. This may yield valuable information, if it turns out that your vendors have more vigorous information security training than you do. That may help you improve your

organization's own security.

How Are They Monitoring Themselves?

Finally, find out what steps the vendor is taking to monitor its own information security. How often do they assess their own security and what do they do to assess it? Do they perform periodic vulnerability testing?

2. Make a Plan: The Vendor Contract

Start with the contract that you already have in place. If you don't have a written contract, you'll need one. Crafting and negotiating contracts with vendors is an enormously complex topic and beyond the scope of this article. Here are some basic categories relevant to information security.

Confidentiality

Maybe this seems obvious, but it's absolutely crucial. Make sure there is a robust confidentiality clause in your contract with the vendor. The vendor must agree, in writing, to keep your organization's confidential information confidential.

Is the Vendor a Business Associate under HIPAA?

If the vendor is a "business associate" under HIPAA, you must have the vendor sign a HIPAA-compliant business associate agreement. Keep in mind that HIPAA imposes certain provisions that all business associate agreements must contain. Make sure your business associate agreements have them.

No Further Use and Minimum Necessary Provisions

HIPAA employs a concept called the "minimum necessary standard." In broad brush, the concept provides that persons must use only the minimum amount of protected health information necessary to accomplish a given task or function. It also means that only persons who need to access protected health information may do so. If you are handling protected health information, this is mandatory. However, organizations are increasingly applying this concept to other forms of confidential information. Law firms are applying the "minimum necessary" concept to their clients' privileged and confidential information. Consider whether such provisions are appropriate in your contracts with vendors.

"No further use" is a related concept. These kinds of provisions state that vendors will not use confidential information for any use beyond the use directly related to the services they are providing for your organization.

Use of Subcontractors

Your vendors have vendors. If your vendors' vendors have access to your confidential information, you should require that you be given advance notice and the right to insist that your vendors' vendors comply with the requirements you have imposed on your vendors.

Your Internal Policies and Procedures

Your vendors need to understand your organization's relevant internal policies and procedures when appropriate. Remember stratification: The company that cleans your office may not need to understand your firm's cybersecurity policies and procedures, but they may need to understand certain aspects of your firm's physical security policies and procedures. For example, if nonemployees are barred from certain areas of your organization's physical plant, the cleaning company needs to know that.

Memorialize any relevant information security rules in the contract and require your vendor to comply with them.[8] Or you could require that the vendor comply with an acceptable third-party information security standard, such as the National Institute of Standards and Technology, International Organization for Standardization 27002, or the SANS Critical Controls.

Requirement to Notify and to Disclose Breaches and Security Incidents

The contract should require your vendor to notify your organization immediately in the event of a security incident — broadly defined — not just in the event of a "breach." You may also want to provide that your organization — and not the vendor — will be the sole judge of whether an incident qualifies as a breach.

Who Owns the Data

The contract should clearly set forth who owns the data. Hint: it should be you, not the vendor, and the vendor should be required to return the data as soon as practicable upon request or to certify its destruction.

Audit Clauses

The contract should permit your organization to audit the vendor's information security processes and procedures. It should also permit physical audits of the vendor's data storage facilities and related controls.

What Happens When the Relationship is Over

The contract should spell out clearly what happens to data in your vendor's possession when the relationship terminates. The vendor should be required to securely return or destroy information in its possession, depending on the circumstances.

What Happens If Something Goes Wrong

The contract should deal with what happens if something goes wrong. One option is an indemnification clause requiring the vendor to indemnify you in the event that the vendor experiences a security incident or breach.

Call Your Lawyer

We've mentioned what is required under HIPAA. But there may be additional requirements imposed by HIPAA and/or other statutes or regulations, depending on the type of confidential information the vendor will be accessing. Call your lawyer. Get advice.

3. Check In: Monitoring Vendor Information Security

The last step in vendor information security is monitoring compliance. This can consist of any number of measures, including as-needed and scheduled reporting, periodic audits, third-party independent reviews, and training and awareness. As with the earlier steps in this process, stratification is key to an effective vendor management program. Some vendors may need little or no monitoring. For others, particularly those that work with your company's confidential information, a more rigorous process may be warranted. Here are some forms of monitoring to consider.

As-Needed Reporting

Reporting is a two-way street. You should update your vendors when your organization changes any internal rules relevant to the tasks being performed by your vendor. And your vendor should report to you any changes in its rules relevant to its task. The vendor should also report on the status of any ongoing efforts, such as vendor employee training and compliance.

Training and Awareness

The best vendor contract in the world won't make a vendor more secure unless the vendor is training its employees and raising their awareness about information security. It may be sufficient for some vendors to simply certify periodically that they are training their employees to comply with any of your organization's relevant information security rules. But for vendors who work with confidential information, you may want to provide the vendors' employees with formal training to ensure compliance with security protocols. To illustrate, law firms sometimes retain "contract attorneys" to review confidential documents produced in litigation. Although contract attorneys generally work on a temporary basis, they may have access to a law firm's systems for weeks or even months at a time. In such instances, training the contract attorneys directly on workstation security protocols and other aspects of the firm's information security rules may be appropriate.

You might also consider engaging your vendors in so-called "tabletop" exercises designed to test breach response preparedness.

Independent Reviews

Consider hiring a reputable third-party review organization such as one of the companies that certify compliance with ISO 27001 to evaluate your vendors. Many organizations are demanding that their vendors with access to privileged and confidential information obtain periodic third-party certification regarding their information security programs.

Regularly Scheduled Checkups

Scheduled reporting — in contrast to as-needed reporting — and scheduled audits or reviews can help ensure vigilance on the part of your vendor. It's good practice to document whatever monitoring activities you implement with your vendors. For vendors that require more vigorous monitoring, put a schedule into place that has dates by which monitoring exercises are to be conducted.

Conclusion

After doing all of the work outlined above for each and every one of your vendors, your reward is two pieces of bad news and one piece of good: You're not secure, and you're not done, but you have moved

the ball forward significantly. The first piece of bad news is not news to anyone who follows data security issues. You cannot guarantee that your organization will not suffer a data breach: All you can do is put in place a reasonable, mindful process to ensure information security. The second is also not news, as you're no doubt aware. Information security requires constant vigilance. What is a reasonable process today will almost certainly be outmoded five years down the road — or even two.

That said, if you follow the conceptual approach set forth above, you will have gone a long way to ensuring that your vendors are not the weak link in your organization's information security chain.

—By David Winters and Andrew Foreman, Butler Rubin Saltarelli & Boyd LLP

David Winters is a partner and Andrew Foreman is an associate at Butler Rubin in Chicago.

[1] This is an oft-repeated data breach "proverb." See, e.g., "Plan ahead: Prepare for the inevitable data breach," Adam Greenberg, available at http://www.scmagazine.com/plan-ahead-prepare-for-the-inevitable-data-breach/article/366348/, and "A Data Breach, It's Not a Matter of If, But When," Ann De Vries, available at http://www.afius.org/page-767462. Throughout this article, we use the term breach as these authors do, in the colloquial sense, not the technical sense under statutes such as HIPAA.

[2] Here is where we would insert a parade of horribles, as is standard procedure in virtually every information security article or seminar we've seen. But most people have heard the horror stories before, so we'll skip the examples. If you are in the mood for morbid subject matter, however, check out the ever-growing list of "Major Incidents" described in the Wikipedia entry for "Data Breach": https://en.wikipedia.org/wiki/Data_breach.

[3] HIPAA refers to the Health Insurance Portability and Accountability Act of 1996, as significantly amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

[4] Gramm–Leach–Bliley is another name for the Financial Services Modernization Act of 1999.

[5] For an example, look no further than the well-publicized incident involving Target Corporation. According to the popular KrebsOnSecurity blog, Target told reporters that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor: a refrigeration, heating and air conditioning subcontractor that had worked at a number of locations at Target and other top retailers. Brian Krebs, "Target Hackers Broke in Via HVAC Company," available at http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/).

[6] At the same time, stratification can be difficult, as the Target breach through its HVAC vendor demonstrated.

[7] "Tabletop exercises" are mock exercises in which the organization involves appropriate stakeholders in a simulation designed to test the effectiveness of the organization's information security policies and procedures. See, e.g., "Breach Preparedness Drills to Test Your Response," by Bob Barker, available at https://iapp.org/news/a/breach-preparedness-drills-to-test-your-response/.

[8] In order to assist with implementing “stratification,” it may be helpful to design your internal policies and procedures in a modular format to facilitate providing only those policies and procedures that the vendor needs to review. For example, if you have a separate policy and procedure that governs access to your organization’s physical facilities, that separate policy and procedure can easily be detached from the larger set of policies and procedures and then shared with those vendors who may need to understand it.
