Bloomberg BNA

Privacy and Security Law Report®

Third Party Vendors

What protections are necessary for companies, and what concessions third party vendors are willing to make in order to secure such companies as customers, will depend on the circumstances, but companies won't get something they don't ask for, so it's vital for companies to know what its ''asks'' should be as they consider negotiating contracts with third party vendors in light of material cybersecurity considerations, the author writes.

Protecting the Data That Matters: Negotiating Third Party Vendor Contracts in an Age of Material Cybersecurity Concerns

By Russell M. Franklin

Introduction

In an age where digitalization is necessary to corporate survival, and public and private institutions are being hacked on what seems to be a daily basis, much has been written on what a company can do to reduce the probability that its sensitive information is compromised as a result of a direct intrusion. However, what is discussed far less frequently is what a company can do to protect the same information when providing all, or a portion of, such sensitive information to third party vendors is necessary for such company's business functions. In reality this circumstance applies to most companies, whether it be in connection with purposes that are tightly tailored to the company's business or something as general as a contract with a cloud storage provider. Regardless of the specifics, in such a situation, a company should be particularly vigilant about the language that appears in its contracts with vendors that will have access to all or part of its sensitive information. The intention of this article is to shed some light on the big picture items that a company should consider as it negotiates a contract with a vendor if cybersecurity issues are a material consideration.

Russell M. Franklin is a partner in Boies, Schiller & Flexner LLP's corporate group in New York and, among other things, has experience in negotiating contracts in light of cybersecurity concerns.

As is the case with any contract, what considerations are deemed material will vary (in nature and significance) depending on the type of engagement, the identity of the vendor, what information the vendor will have access to and how that information will be accessed. Accordingly, what concepts are reflected in such a contract, and how, has to be determined on a case-by-case basis with a particular eye towards the circumstances. That said, if cybersecurity issues are a material concern, there are a few concepts that are important enough (and general enough) to warrant consideration regardless of the specific circumstances surrounding a vendor contract. These concepts include:

1. an ironclad confidentiality provision;

 ISSN 1538-3423

2. appropriate representations and covenants with respect to the existence of, and maintenance of, sufficient security protocols;

3. the company having a right to effect a physical audit on the vendor's property to confirm how such company's sensitive information is being used and what security protocols are in place to protect it;

4. the company having a right to terminate the contract upon a material data breach (even if such data breach does not expose any of the company's information);

5. an appropriate indemnity to make the company whole in the event that the company is harmed as a result of a data breach; and

6. restrictions on publicity.

Each of the aforementioned considerations are discussed in more detail below.

Material Considerations

An ironclad confidentiality provision that limits the use of ''confidential information'' to those purposes that are absolutely necessary for the vendor to provide the applicable services.

Although some consider confidentiality provisions to be ''boilerplate,'' substantial thought should be given to the language contained therein if cybersecurity concerns are present. For example, in this case, the language has to be drafted such that both a voluntary and involuntary (i.e. a forceful intrusion) sharing of confidential information would result in a breach of the confidentiality provision.

A company should strive to use vendors that do not have to provide a company's sensitive information to yet another third party in order to provide the requisite services.

When it's necessary for a company to provide its sensitive information to a vendor in order for such vendor to provide services, a company should strive to use vendors that do not have to provide a company's sensitive information to yet another third party in order to provide the requisite services. In the event that everything is handled in house, the contract should expressly state that, subject to legally required disclosures, confidential information will not be provided to a third party without the company's consent.

If a vendor must provide certain sensitive information to a third party in order to provide the services in question, the company should be certain that it understands (and the contract expressly states) who such information will be provided to and for what purpose. Given that each additional entity that has access to such information translates into additional risks, the objective is to limit access as much as possible.

If a vendor must share a company's sensitive information with a third party in order to provide the requisite services, each applicable third party should be subject to a confidentiality obligation that is at least as restrictive as the one between the company and the vendor. If possible under the circumstances, it is also worth considering if the company should be an express third party beneficiary of such confidentiality obligation. Leaving aside what the confidentiality provision between the vendor and its related parties says, the vendor always should be directly liable for any breach of the confidentiality provision that appears in the contract between the vendor and the company, even if one of the vendor's related parties is the entity that is ultimately responsible for such breach.

Regardless of if the vendor is a one-stop-shop, or one that leverages a network of other entities to provide the requisite services, a company's sensitive information only should be viewable by employees of such vendor (or related parties) that need to access such information in order for the vendor to provide the services in question—and such sensitive information only should be used in connection with the provision of such services. Both of these requirements should be express in the contract, as, if they are not, it is often the case that any employee of the vendor (or of a related party), whether working on the engagement or not, could view such company's sensitive information and, so long as such information is not provided to a third party, use such information for a myriad of purposes (for example, internal marketing research purposes), all without being in breach of the terms of the contract.

Inclusion of material representations about the security protocols the vendor currently uses to prevent data breaches, and covenants that ensure that, as technologies advance, the vendor appropriately updates its security protocols.

Every company with cybersecurity concerns does some homework on a potential vendor's security protocols prior to engaging such vendor. However, reviewing the security protocols that a vendor advertises on its website or includes in its pitch materials is an insufficient method of ensuring that the vendor's security protocols are adequate. If particularly sensitive information will be shared with the vendor, it may be fruitful to visit the vendor's facilities to see firsthand what security protocols are being utilized at the time and how they are being implemented. Yet, even if the nature of the information that will be shared does not merit a site visit, a vendor should have no objection to formally representing, in one form or another, in the relevant agreement that it utilizes and appropriately maintains the security protocols that it advertises it uses. The existence of this representation and warranty provides the company with a remedy if it is later revealed that, at the time the representation was made, the vendor did not actually conduct its business in the manner it advertised.

  PVLR ISSN 1538-3423

An audit right is a particularly difficult right to acquire, but if a company can negotiate for such a right, it always will provide a company with more information than it would have access to in its absence.

Because vendor contracts can survive indefinitely, the aforementioned representation is necessary but not sufficient since representations are made as of a fixed point in time. Accordingly, a company also would want contractual assurances (in the form of covenants) that the vendor's cybersecurity measures will advance with the times as the relationship progresses. In both cases, the remedy associated with a breach of the representation or the covenant will be vital. Indeed, if noncompliance is severe enough, the company should have the right to immediately sever the relationship (without penalty) and promptly receive its sensitive data back[1].

The inclusion of an ''audit right'' that allows the company to visit the vendor's premises and inspect the security protocols that are being implemented at the time.

Assuring that sensitive information doesn't fall into the wrong hands has monetary value to every company. Yet, in the case of a company that provides sensitive information to a vendor, there is no contractual provision that can provide real time insight into (i) how a vendor is actually using such company's sensitive information or (ii) what measures the vendor is utilizing to ensure that such information doesn't fall into the wrong hands. If a company needs to know this information, only an audit right can provide it. That said, an audit right provides little value to a company if it isn't coupled with an appropriate remedy. In this case as well, if noncompliance is severe enough, the company should have the right to immediately sever the relationship (without penalty) and promptly receive its sensitive data back.

Because an audit right requires entering another company's physical space, if an audit can be conducted at all, there are always material restrictions on how and when they can be conducted. Typically there are also restrictions on the frequency in which they may be conducted (generally once a year).

[1] Although beyond the scope of this article, it is worth noting that there are often situations in which it is not possible for a vendor to return (or destroy) all of a company's sensitive information. This may be due to the fact that a copy must be kept for compliance reasons, because of logistical challenges associated with how such data was stored and/or used, etc.

In the event of a material data breach, the company should be able to immediately terminate the vendor contract (without penalty) and promptly receive its sensitive data from the vendor.

An audit right is a particularly difficult right to acquire. That said, if a company can negotiate for such a right, regardless of how restrictive the audit right ends up being in final documentation, it always will provide a company with more information than it would have access to in its absence.

The ability to terminate the contract in the event that the vendor is the subject of a material data breach, even if such breach does not impact the company's data.

In today's ultra-competitive environment, many vendors have to provide services for some minimum term (usually 12 months) in order to make a profit. With that in mind, in an effort to ensure that such contracts are not easily terminable, such contracts generally are only terminable upon a material breach. Typically what counts as a ''material breach'' isn't specifically defined.

Although quite common, this construct is particularly problematic from a cybersecurity perspective for at least two reasons. First, it often takes a material amount of time to uncover exactly what data has been exposed in the case of a data breach. Second, even after a company that is a client of a vendor that is the subject of a material data breach can confirm that a portion of its data has been exposed, in order to terminate the contract pursuant to its terms, the company still must successfully demonstrate that such a breach amounts to a ''material breach'' of the contract.

For reputational reasons, any company that has shared sensitive information with a vendor that is the subject of a material data breach (whether or not such breach exposed all, or any portion of, the company's sensitive information) would prefer to be able to tell its clients that it promptly severed ties with such vendor to maintain (or begin the process of rebuilding) client confidence. This simply is not possible if the company must demonstrate a material breach of the contract before it can distance itself from such vendor.

Accordingly, a company should look to clearly define what will count as a ''material data breach'' and ensure that the company is privy to a specific remedy in the event that the vendor becomes the subject of a material data breach. Ideally, in the event of a material data breach, the company should be able to immediately terminate the vendor contract (without penalty) and promptly receive its sensitive data from the vendor.

An appropriate indemnity to make the company whole in the event that a data breach does expose the company's sensitive information.

In an effort to keep their pricing as competitive as possible (which requires being able to reasonably predict the financial exposure associated with each contract), most vendors include a blanket limitation of liability with no exceptions in their contracts. However, there are a number of exceptions to a blanket limitation

on liability that are appropriate, and a breach of the confidentiality provision is one.[2] Vendors are quick to remind a company that, regardless of what precautions the vendor takes, there is nothing it can do to ensure that its systems will not be compromised. This, of course, is irrefutable. However, from an allocation of risks standpoint, it is also most appropriate for the vendor to assume all, or a material portion of, that risk since the vendor determines what checks and balances it imposes with respect to the protection of its systems. Ultimately, in the case of a breach of the confidentiality provision (whether as a result of a data breach or otherwise), the indemnity should allow the company to recover its losses from dollar one without a cap.

Restrictions on Publicity

Vendors like to promote who their clients are in an effort to encourage other notable companies to use them as well. Vendors are often granted the right to do so pursuant to a publicity provision. As a general matter, material thought should be given to this provision as, sensitive data aside, most companies would like to approve how their name and logo are used, and under what circumstances. Yet, companies should be particularly wary of letting vendors use such company's name for advertising purposes if such vendor possess any of the company's sensitive information as, from a cybersecurity prospective, having a vendor publish who its clients are provides hackers who are looking to exploit a particular company's sensitive information with a road map as to where to look to do so. This is particularly true if the company's security protocols are superior to those of the vendor in question. In such a case, a direct attack may be less attractive than an indirect one.

Conclusion

Although it is impossible for a company that shares sensitive information with vendors to ensure that such sensitive information will remain confidential under all circumstances, there are steps that a company can take to minimize the probability of an indirect data breach and, in the event that a vendor that such company uses becomes the subject of a data breach, ensure that it can quickly mitigate the damage and recover any and all losses it may incur as a result of such data breach. This article has touched upon some of the more generally applicable ways to do so.

Ultimately, what protections are necessary for the company, and what concessions the vendor is willing to make in order to secure such company as a customer, will depend on the circumstances. However, since a company won't get something it doesn't ask for, it's vital for a company to know what its ''asks'' should be as it considers negotiating contracts with third party vendors in light of material cybersecurity considerations.

[2] Another exception that is particularly important relates to intellectual property. If the vendor misappropriates the company's intellectual property, losses associated with that breach should be excluded from the limitation of liability. Similarly, if it turns out that the vendor's product infringes on the intellectual property rights of a third party, any losses that the company incurs in connection therewith also should be excluded from the limitation of liability.

  PVLR ISSN 1538-3423