CYBERSECURITY LAW & STRATEGY

SEPTEMBER 2017

Vendor Contracting for Privacy and Security

By Chuck Kunz and Ian McCauley

In an effort to continue to capture ongoing and new business, vendors may be opening themselves up to liability due to poorly drafted contracts with companies. In addition, in a rush by companies to have data shifted to the cloud, privacy concerns may be dangerously minimized.

It is difficult to deny that data security and privacy issues are now at the forefront of business concerns. Many businesses are now highly attuned to the risks of exposing their own or their clients' protected information due to well-publicized massive hacks of medical or consumer information over the past several years. These businesses are now taking very aggressive steps to limit the risk of hacks, malware, ransomware and other intrusions into their own systems.

An additional consideration is now in play; information that may reside with businesses' vendors or other service providers. Recent experience suggests companies are just as demanding (if not more so) when it comes to their vendors and vendor agreements. Indeed, many proposed vendor contracts seek the wholesale shift of risk from the data owner to the data vendor through hold-harmless and indemnity provisions. Experience also suggests there is little thought, however, being given to the effectiveness of the vendor's security systems, or the types of information to which the vendor may be privy.

In many instances, it appears that companies are simply trying to "check the box" in order to show that they have a vendor agreement and a potential avenue of collection and indemnification should the vendor suffer a breach. Vendors, on the other hand, can — and must — push back on the onerous terms of some of the privacy and security demands being made by companies.

Scenario 1

Vendor has done business with Company for several years pursuant to a five-page written contract. In financial terms, the contract is fairly minor, but the Vendor hopes that continuing to do business with Company will lead to additional business in the future. This year, Company sends Vendor a renewal contract, but for the first time includes a nine-page "Privacy and Security Addendum" to which Vendor is asked to assent for the contract to continue.

Among other things, the addendum requires Vendor to immediately notify Company of any attempted access to Vendor's computer systems regardless of whether Company's information was at risk, requires Vendor to hold harmless and indemnify Company for any breach impacting the Company's information, and requires Vendor to have certain types of system security. Vendor must also communicate through an encrypted network, would be required to have documented training of all employees, and be subject to periodic audit by Company of its data security and privacy practices. Company also desires the right to have its own scans of Vendor's systems performed, and Vendor must agree to comply with "All Laws" that govern privacy and data security anywhere in the world.

Faced with the risk of losing Company's current and potentially future business, there is a very real risk that Vendor will simply sign such an agreement. Many vendors may close their eyes, sign the contract, and hope nothing happens. But Vendor can and should attempt to negotiate a reasonable addendum that makes sense both from a privacy and data security standpoint and also from the position of what can reasonably be requested from the Vendor.

Considerations

In the scenario above, Vendor should take a careful look at several things.

What law governs the contract vs. the Privacy and Security Addendum?

Choice of law is always a critical component of any contract. Privacy and data security issues can impact many state and federal laws. There may rightfully be a particular state's law governing interpretation and enforcement of the contract, and a request by Company for Vendor to adhere to certain laws can be appropriate. But adherence to "All Laws" could conceivably put Vendor in breach as soon as the contract is signed as it's likely impossible to comply with "All Laws." Company may be seeking that Vendor comply with "All Laws" as a way of shifting potential liability for a data breach and breach notification onto the Vendor. So, consequently, Vendor should exercise caution when evaluating a contract that would greatly expand its compliance obligations. Under state breach notification statutes, Vendors often have notice obligations to Company, but not necessarily to the actual person whose data has been accessed. Vendors should be careful not to take on independent notification obligations via a contract requiring compliance with All Laws.

Vendor should also be concerned about whether the data being provided to the Vendor impacts international privacy laws governing international data transfers. Will Vendor need to comply with the General Data Protection Regulation? Or the Payment Card Industry Data Security Standard? If not, Vendor should carve such provisions out of any agreement. Vendor should not agree to comply with laws that may have very stringent privacy policy implications and personnel requirements. In short, a vendor contract should be limited to actual laws that may impact the privacy and security of the types and character of the data being handled.

What are the security obligations that will be required from the Vendor, and what is the Vendor doing now?

When evaluating an agreement, Vendor should be prepared to discuss what protections it already provides for its own information and what it can and will do to protect the information of its customer. In many instances, Company may request that Vendor undertake significant system advances at significant costs that Vendor may not be financially able (or willing) to implement. An open discussion of the current capabilities of Vendor and what it might already be doing (*i.e.*, firewalls, password management, and patch management), or can reasonably do with minimal additional investment in technology (*i.e.*, encryption, device management, intrusion detection), can sometimes lead to a more rational data privacy and security solution for Company and Vendor alike. But Vendor has to know what it can and cannot do, and must be able to convince Company that it can meet the spirit, if not the letter, of what Company desires.

What will the Vendor's obligations be in the event a breach is discovered?

Undoubtedly, because of potential breach notification obligations, Company wants to be notified of a breach promptly. Sometimes, Company's desire comes with demands that notification from Vendor be made "immediately" or "within 24 hours." Sometimes, the demand is without regard to whether Company information is implicated.

Often, these onerous demands can be negotiated to something more agreeable, such as requiring notice within a reasonable time after discovering that a breach has impacted Company's information. Company might also require that Vendor provide it with a written description of the alleged breach, a copy of any analysis or report that might have been drafted regarding the breach, a description of corrective action that has been taken, and an assessment of the risk to Company. Parties should carefully draft such provisions to assure that Vendor is not inadvertently

agreeing to waive attorney/client or attorney work product privileges, or otherwise contractually agreeing to allow the customer access to confidential reports.

Vendor should also consider who directs the scope of breach remediation, and what remediation might be appropriate. For example, Company's proposed agreement may require Vendor to take all necessary and appropriate remediation at the direction of Company, but at Vendor's cost. It may require Vendor to retain lawyers to prepare breach notices for Company at Vendor's expense, and for Vendor to bear the cost of sending all required notifications. And virtually every agreement attempts to require Vendor to hold Company harmless and indemnify Company for any damages. This type of provision allows Company access to Vendor's checkbook and such broad language should be avoided, or at least strictly curtailed.

As previously noted, there is always a risk that Vendor may merely sign an onerous agreement, or may not feel as if it has negotiating leverage when dealing with Company. But there are currently some areas that can and should be negotiated when it comes to vendor agreements addressing data security and privacy concerns. The reality is, however, that while some vendors may be able to negotiate a workable solution with their customer, others may not be able to do so. At those times, the vendor may have to make the hard choice to close its eyes and sign, or decline to enter the contract.

Scenario 2

Company wishes to have its data hosted offsite. Host provides Company with a proposed hosting agreement that effectively disclaims all liability to Company in the event Host suffers a breach impacting Company's data, or if Host is unable to provide access to Company's data due to a denial of service event or other interruption in service. Host has not been in business all that long, but an investigation by Company suggests that others have had a good experience with Host, and Company wishes to engage Host if appropriate changes can be made to the agreement. In this scenario, Company, as the buyer of Host's services, likely has more bargaining power. It can seek hosting services elsewhere. Therefore, Company can likely push for more favorable terms from Host and should consider some of the following things.

Is Host financially sound?

The nightmare scenario in any type of data offloading is the possibility of Host holding Company's data hostage. Before providing data to Host, Company should do some independent investigation of Host's financial wherewithal. This may include an evaluation of Host's finances, Host's relationship with its landlord, if any, and Host's ability to perform under the contract. It may require an investigation into Host's relationship with its other creditors. Provision should be made within the contract about data ownership and continued access in the event of Host's insolvency, with the key being for Host to provide Company with continued access to information at all times.

Where is data being hosted?

Company will want to include representations and warranties about where Company's data is being hosted. Are the servers located in the United States? Are they located outside the United States, and if so, where? Issues abound with respect to information ownership when data is hosted elsewhere, and Company should take careful note of where its data resides.

What is Host's plan in the event of a breach affecting Company's data?

Just as Company should have an incident response plan if its systems are breached, Host should also have one, and Company should ask to see it. Making sure that Host has a workable plan,

and the means to implement it, will help assure Company that Host is prepared to appropriately respond to a breach, including discovery, recovery and remediation.

Company should also negotiate a requirement that Host provide prompt notification of any attempted breach of Host's system that might affect Companies' information. This allows Company to evaluate the breach, and determine whether it may have breach notification obligations.

What practical protections does Host have in place to prevent breaches?

What firewalls, intrusion detection/protection management, and system segregations are in place to protect Company's information? Will Company's information be hosted on the same servers that host others' information? Who will have access to Company's information and for what purposes? What records or logs will be created when the servers hosting Company's information are accessed for updates, patches or general maintenance, and who will have access to Company's information and under what circumstances? Understanding and evaluating Host's own proactive steps and readiness in the event of a breach is critical. Company should also be wary of Host's desire to use "commercially reasonable efforts" to prevent unauthorized access to Company's data. Given the minute-by-minute advances in technology, consider instead negotiating with Host to require comply with "industry standards" or "industry best efforts."

Does Host utilize third-party providers?

Company should determine what third-party providers Host uses to provide the services and what Host's agreements are with those third parties. It is not uncommon for Host to attempt to disclaim any warranties with respect to the third-party services being utilized by Host. It is important to consider what third-party services might impact Host's provision of services to Company, and whether Host has taken appropriate measure to assure continuation of services even if a third-party provider fails to perform.

Has Host attempted to limit liability?

Frequently a Host may attempt to limit liability to the Company through provisions limiting the types and amounts of damages, adjustment to statutes of limitation on asserting claims, and otherwise seeking indemnity from the Company. A Company should carefully consider the language and extent of any limitation of liability or recourse to Host, and may be able to negotiate significant reductions in proposed limitations. As an additional consideration, Company should also confirm that Host has appropriate insurance policies in place, including cyber-liability insurance in sufficient amounts.

Are there reasonable termination provisions?

Hosts may attempt to limit a Company's ability to terminate the agreement. Some include provisions limiting early termination for any reason. Others allow for termination for cause with an opportunity to cure. Many include automatic renewal provisions. Company should evaluate whether it is comfortable with automatic renewals at regular intervals and at pre-determined pricing. Termination provisions usually can and should be negotiated to allow termination under reasonable circumstances with or without cause. This might include longer notice provisions if there is no cause, and shorter, or immediate termination where cause exists.

When and how does Company retrieve its information (or transition its information to another provider) upon termination?

A fundamental consideration in any hosting agreement is how Company transitions its information to a third party at the conclusion of the contract, and how long Host must continue to host the information until the seamless transfer can be completed. While transitioning such services may include additional costs to Company and an additional fee to Host, the provision of transition services should be discussed and fleshed out in any agreement. And the transition period should be sufficient to assure that the information is operational at the new host before the services are shut down — and the information destroyed — by the old Host.

Negotiation of hosting agreements should not be taken lightly. Companies should keep in mind that they are providing some of their most critical information to a third party and should plan to protect it accordingly. This means protecting it when it's hosted, having full time access to it, and getting it back intact. Along the way, companies should assure that their hosts are taking appropriate steps to protect the integrity of the information, and providing prompt notice when things go wrong.

Conclusion

Whether one is purchasing services or providing them, data security and privacy issues should be paramount considerations. Currently, many vendor-related contracts can be negotiated, and parties should take the opportunity to do so when available. In order to best position themselves for a negotiation, parties should continually evaluate their own privacy and security measures so when they are negotiating they can easily assess what they can and cannot do. Only then can they avoid being shut out of the market, or worse, signing an agreement with little understanding of the potential risk.

*****

Carl N. "Chuck" Kunz, III, is a partner with Morris James LLP in Wilmington, DE, where he chairs the Data Privacy and Information Governance Group. He also is a member of the firm's Bankruptcy and Creditors' Rights Group. **Ian D. McCauley** is an associate with Morris James LLP, where he serves as the firm's eDiscovery Coordinator. He also provides advice on information governance and data privacy.