Barclay Damon Live Presents *Cyber Sip™*
Season 5, Episode 1: "Data Privacy and Vendor Agreements: Five Negotiating Points"

Host: Kevin Szczepanski, Barclay Damon

[Kevin Szczepanski]: Hey everyone, it's Season 5, Episode 1 of Cyber Sip. And we're also in Data Privacy Week. So today's episode is going to focus on data privacy and vendor agreements. And I'm going to run down five negotiating tips that I think will be pivotal for you in negotiating your vendor agreements. Why is this important? Let's start with that. Well, as an organization, you undoubtedly have your own set of data privacy and security controls in place to protect your data and your computer system. But if, like many organizations out there, you're using vendors to deliver your services. You need to make sure that your own data privacy and security controls flow down to each vendor, partner, and service provider you use. Otherwise, you've got gaps in security that could result in risk and liability for you, and you want to avoid that whenever possible. So it's with that in mind that I want to cover five negotiating points. Let me run down what they are. And then I want to give you a quick overview of what I've been seeing in vendor agreements.

[Kevin]: So the points we're going to cover are data use terms, data security requirements, auto renewals and termination, indemnification, and insurance. But before we cover those five negotiating points, I just want to begin with a quick overview of vendor agreements. They can be vague. And what I mean is that very often you can read a vendor agreement and not know exactly what the vendor is promising to do, what the vendor's responsibilities are, what the vendor is going to do if it breaches the agreement, and what your rights and responsibilities are. So, step number one with any vendor agreement is to pass that along to the appropriate person, the lawyer in your organization or out to give that document a read and give you the best sense of whether this is something that can serve as the basis of your agreement.

[Kevin]: I can tell you, I saw one vendor agreement recently that we ended up telling our client, you know, this isn't really even an agreement. It was a one-page document with 17 paragraphs, and it was titled an agreement. But really it was just a list of the 17 things that the vendor wanted the customer to do, and the vendor wanted the customer to be responsible for. No specifics as to services, no provisions covering data security, indemnification, insurance, none of that. So we ended up looking at that again, saying, not only is this vague, but it's not really even an agreement. So obviously there are a lot of considerations that go into vendor agreements. There's also the balance of power. How can you negotiate what you really want in a vendor agreement if you're dealing with a large national vendor and your smaller organization. You might not have the negotiating power. We'll talk a little bit about that along the way. The takeaway is we do our best to deliver the most robust protective provisions that we can. Sometimes we get everything we want. Very often we don't, but we do our best along the way. So with that, let's dive right in to the five negotiating points we're going to cover today.

[Kevin]: Number one: data use terms. Let's run down those and you'll see what we mean. First your vendor agreement should clearly spell out the data that the vendor will access to perform services. Only that data that's necessary should be turned over to the vendor and only those individuals within the vendor's organization who are performing services should have access to it. So we want to tighten it up both as to the nature of the data and the individuals that will be allowed to access it.

[Kevin]: The second negotiating point I'd like to share with you is data security requirements. You want to make sure that your vendor is bound to maintain reasonable security standards. What does that mean? Well, you can find reasonable security standards in a relevant statute or regulation. If you're not bound by applicable law, you might turn to an industry standard such as NIST. And NIST provides many helpful security standards on an industry by industry basis that maybe, standards that apply in the financial industry, that may apply in the health care industry. That's another source of a potential standard. Or in a perfect world, you can include in your vendor agreement a specific data security provision or addendum that spells out each and every requirement with which you want your vendor to comply. And that's especially important in a case where your organization is already a vendor to your customer, and your customer agreement may require you to comply with data security standards and may even require you to cause your vendors to comply with … those same standards. So you're in a situation where your customer requires you to comply with a specific set of data security standards. You want to make sure your vendor is bound to those same standards. Otherwise, you have a gap in security. And as between you and your customer, you're responsible for that gap.

[Kevin]: The third negotiating point I want to talk to you about concerns auto renewals and termination. You probably know very many of these vendor agreements, there are auto renewal provisions, essentially saying that unless you or we cancel, the vendor agreement is automatically renewed at the end of the contract period. Now, that may sound convenient. And it may be very good for the vendor but suppose that your vendor agreement auto renews. And in the second month of that renewal period, you decide you need a new vendor. You need to move into a different direction. You may be stuck with ten months of fees that you will owe the vendor after termination. So how do we want to address this? We want to first scour the agreement for any actual or hidden auto renewal provisions. Some…what do I mean by "hidden"? Instead of saying unless we otherwise agree, this agreement will auto renew, some of the auto renewal provisions are a little bit more subtle. They may say "this agreement will automatically renew upon the inclusion of an additional service." So you may not realize that six months into your agreement, the vendor is providing an additional service it did not provide on day one. And if you don't read the fine print, you don't realize that now you don't have six months left on that contract. You have 12 months left on that contract, and that can be problematic. We've seen disputes arise when the client wants to cancel a vendor agreement, and finds out either that it cannot or that it cannot without paying significant termination fees. Now, sometimes you may want… it might be worth it to pay those termination fees because it's more important to switch to a new vendor than it is to avoid the cost of termination. But whenever you can, you want to bargain for a very simple, straightforward provision that allows you or either party to terminate with or without cause on certain notice. It could be 30 days, it could be 60 days. That's a subject of negotiation, but that's the ideal termination provision. You want to avoid auto renewal whenever possible.

[Kevin]: Negotiating tip 4: indemnification. So here's how I think of it. Each side has things to do. Each side has services or obligations under the agreement. What happens when one side… your vendor fails to do what it promises to do? It can result in a loss. It can result in a claim being made against you for something your vendor did that resulted in a breach of privacy or security. The answer to that is "indemnification." You want a provision in the agreement that shifts the risk to your vendor if something your vendor does or doesn't do causes a loss or a claim against you. Now the vendor might turn around and, you know, assuming they don't say "no." We know these indemnification provisions exist. So very often they do say yes. But what they'll say is we want you to indemnify us as well. And you may be reluctant to do that, but that's okay. Sometimes that's the price of poker. In order to get indemnification, you have to give indemnification. But here's the thing. You can control what you do or not do. So from your perspective, indemnification might not be a heavy lift, but you can't control what your vendor does or doesn't do. So if you have to offer indemnification in exchange for getting it from your vendor, that's the right idea.

[Kevin]: Bilateral indemnification is not only doable, but in my view, it's critical, especially when we get to the fifth negotiating point, which is insurance. Why is this so important? And I know many of you have general liability, cyber, errors and omissions, but some of you don't and some of you don't think it's necessary. But here's the thing. All the indemnification in the world running from your vendor to you will not help you, if, at the end of the day, your vendor does not have the financial ability to defend or indemnify you for a judgment in a civil case or a settlement you might have to make as a result of a claim against you. So the solution to that is requiring your vendor to maintain insurance and name you as an additional insured. What types of insurance are important? At a minimum, you want your vendor to maintain general liability insurance, errors and omissions insurance, and cyber insurance. Adding to that, you want, if at all possible, your vendor to maintain umbrella insurance so that there is a layer of coverage over and above the limits of your GL, E&O, and cyber insurance by requiring your vendor to have that appropriate insurance in place, you secure, in effect, the vendor's indemnification obligations and you further protect yourself.

[Kevin]: So those are the five negotiating points I wanted to share with you here in Data Privacy Week. There are many more negotiating points that we could discuss. We haven't talked about limitation of liability provisions, which you need to excise if you can, and if you want to limit your own liability, you might have to limit your vendor's liability. But if your vendor does something wrong and it results in a data breach that requires you to expend hundreds of thousands of dollars investigating, giving notice, and defending a data breach class action you don't want a limitation of liability provision that's going to limit your recovery to the last three months or six months of monthly fees. That's not going to cut it. So that's an important bonus negotiating points that you want to think about as well. So whether it is data use terms, data security requirements, indemnification, insurance, and auto renewals and termination, there are many important lines of focus.

[Kevin]: So I hope this rundown of negotiating points for vendor agreements is helpful to you. If you disagree with something you've heard, or if you have another provision in mind that we didn't talk about in this episode, hit me up in the comments or contact me. You have my contact information. I'd love to hear from you, because this is an ongoing process and we're all just trying to get by and improve and do the best we can. So happy Data Privacy week! Hope you enjoyed Season 5, Episode 1 of Cyber Sip, and stay with us because we're back soon with another episode.