Barclay Damon Live Presents *Cyber Sip™*

Season 5, Episode 10: "The AI Vendor Contract Trap: What Businesses Miss Before Signing, Part 1"

Host: Kevin Szczepanski, Barclay Damon

[Kevin Szczepanski]: Welcome back, everyone. Today we're talking about the AI vendor contract trap. So you found the perfect new AI platform, and you need it. The demo was incredible. Your entire team is thrilled. And not for nothing. But the vendor is offering a steep discount. Maybe 50 percent if you sign before the end of the quarter. So everyone is happy, and everyone wants to move fast. Technology promises to automate workflows, reduce costs, improve efficiency, and maybe, maybe especially, give your company a competitive edge. So you're ready to move forward, and you need to do it lickety-split. Then the contract itself shows up, and somewhere in the middle of all that fine print, you (or your lawyer) realize that something isn't quite right. You see, if something goes wrong in the delivery of services, they're late, you suffer a loss, or worse yet, the AI malfunctions and you suffer a data breach or a privacy lawsuit, you own it. The vendor, on the other hand, may have no meaningful responsibility at all. In fact, the agreement may require your company to absorb most of the risk.

[Kevin]: Welcome to modern vendor contracting. Today on *Cyber Sip*, we're going to talk about vendor contracts, what the risks are, why they exist, and how you can protect yourself without losing the opportunity to innovate. Because as companies race to adopt AI, biometrics, automation tools, and predictive analytics, one of the biggest risks is often not the technology itself—it's the contract behind it. So let's start with the rush to adopt new technology. And it's understandable because businesses today are moving incredibly quickly to adopt those technologies. We're seeing organizations implement AI customer service platforms, AI-powered document review systems, biometric timekeeping tools using fingerprints or facial recognition, automated HR and hiring systems, predictive analytics tool, employee monitoring software, and even cloud-based healthcare and financial technologies. And of course, many of these technologies are extremely valuable. They can eliminate repetitive work, streamline your operations, improve your customer experiences, and create substantial efficiencies across the platform. Many of these technologies might even be required by agreements you have with your clients or customers. We've seen that too. We've seen our clients dealing with agreements in which they are required to adopt AI, biometric technology. So the choice has already been made for them. But here's the thing. These technologies can also create new categories of legal, operational, and cybersecurity risk because many of them involve the processing and use of highly sensitive information. Customer records. Employee data, biometric identifiers, financial information, health care information, trade secrets, you name it.

[Kevin]: It's all in play. And in the excitement surrounding this new technology businesses sometimes overlook one critical issue: whether the contract actually protects them if something goes wrong. And that's very important. Many modern vendor agreements, though, are not really balanced agreements at all. We've seen vendor contracts that are heavily one-sided documents that are drafted to limit the vendor's exposure, while shifting much of the risk to you. Let me give you an example. I recently reviewed an agreement involving a new technology vendor that was so one-sided it barely resembled a contract. The contract was literally a page or page-and-a-half of very small, densely set paragraphs that, if you read them, really didn't promise anything. The vendor told you what it wouldn't do and what you were responsible for. But as far as the actual scope of work, not so much. And no provisions for data security, indemnification, or insurance. That's a problem. That's a contract that you want to avoid or that you need to revise in order to make it work. In other words, no accountability on the vendor's part if something were to go wrong or if sensitive data were compromised. Now, the client was understandably very excited about the technology and wanted

to move very quickly to secure favorable pricing. But when we stepped back and we talked with the client about the agreement, we were able to point out some potentially significant risk. And the client's reaction was, okay, we want the services, we need the technology, but we're not going to sign just anything. We're going to have to make this agreement work for us, as well as the vendor.

[Kevin]: And that's really what we're going to talk about today. How do you deal with a situation where you want the technology, you need the services, but you can't deal with the contract? We're going to talk about that now. And the first question we're going to grapple with is the sometimes-thorny question of whether you should work with and revise the vendor's agreement, or you should replace it entirely with your own paper. And as you can imagine, the answer depends on the situation. If the agreement is just like the one I told you about, it's probably best to start from scratch or use your own form. It'll feel less like you're doing a complete rewrite and more like you just prefer your own paper. If you're working with an established vendor who has a better form, chances are the vendor will want to use its own form. It will be generally workable at least, and you can redline your own changes. Either way, your vendor is probably going to want to disclaim warranties, limit its liability, and shift as much of the risk away from itself as possible. Now, does that mean negotiation is going to be difficult? Does that mean you're going to be fighting with your vendor before you've even started the relationship? No.

[Kevin]: Most vendors are going to be ready, willing and able to negotiate to a point. And after all, you're trying to get off on the right foot with what you hope will be a productive, successful relationship by treating your future business partner like a partner and not like an adversary. So ultimately, what we're thinking when we help our clients with these vendor contracts is not that we want to "win" the contract negotiation. The goal, instead, is to create a win-win agreement that works for both sides. So with that in mind, let's turn to some of the key contract provisions that you should focus on. So let's begin with the scope of work. Clearly one of the most important parts of the contract. You want to understand what the vendor is actually going to do. What services will it be providing? What product will you receive? And yet, I have to say this is one of the more overlooked parts of the contract. Routinely, we see contracts with a scope of work that's empty or for which there isn't even a provision. That's a problem.

[Kevin]: And you would think it wouldn't be. We think this would be very basic, but a lot of times when vendors and you are negotiating on the fly, you leave this important piece out. And yet it becomes critically important when you're dealing with AI systems and emerging technologies, because misunderstandings about data use, functionality, and responsibilities on both sides can lead to problems later. So you need to understand exactly what services the vendor is providing, what data the vendor will access to perform those services, whether the vendor is going to have subcontractors or third parties involved in providing those services, and what the vendor intends to do with whatever data you might provide it to perform the work. Sometimes vendors will use it solely to perform the services. Other times, vendors try to reserve in the fine print the right to use the information that you provide them to train their model, or for marketing or other business development reasons. Critically important that you understand up front what the vendor will do, won't do, and of course, what the price is for those services.

[Kevin]: The next item I want to talk to you about is cyber security, obligations, and compliance. This is where many agreements become comically and sometimes dangerously vague. You'll often see language stating that the vendor will maintain, "commercially reasonable security measures." Now, that might sound good and maybe even reassuring...until there's a breach and everyone starts to debate what "commercially reasonable" actually means. A stronger agreement gets far more specific. Organizations should understand whether the vendor maintains a written information security program. Whether the vendor has adequate security controls in place. Is the vendor using MFA? Is the data encrypted? What other administrative, physical, and technical safeguards will the vendor use?

[Kevin]: Does the vendor regularly assess its own security through assessments or penetration testing, vulnerability scans? Does the vendor have a formal incident response plan? When are you going to learn that the vendor has experienced a data or security breach? Will it be as soon as reasonably possible, or will it be within 24, 48 hours? Because in the middle of a ransomware attack, hours actually matter. And your organization should also evaluate whether the vendor is in compliance with applicable laws and recognized frameworks. Some examples would be the FTC safeguards rule for some financial businesses, state privacy laws, such as the New York State Department of

Financial Services Cybersecurity Rule. And if it is a health care provider, will the vendor also represent its compliance with recognized industry security standards, such as the National Institute of Standards and Technologies or other ISO-based frameworks? And here's something that businesses sometimes miss entirely. A vendor may make the best and most convincing representations during the sales process about its security and its compliance with applicable law. The marketing materials, the salesmanship may sound fantastic, and it may be well intentioned. A sales team may promise enterprise-grade protection, for example. But if those representations, if those commitments never actually make it into the contract itself, enforcing them later will become much more difficult. As one of my partners often says, "If it's not in writing, it didn't happen." And that concept works in the vendor contract negotiation process as well. If what you want and what you don't want isn't spelled out clearly in the agreement, you're not going to be able to enforce it later. And there are special rules for AI agreements as well. You're going to want to know what the vendor does with your prompts, the information that you input into the software, what your vendor does with the results—are those prompts and results used to train the vendor's model?

[Kevin]: Are they or can they be shared with third parties such as business or marketing consultants? Will they be shared with government entities under any circumstances? Too often there's no discussion about this up front. And in our experience, clients then can become surprised and maybe even harmed by something that happens to their data or to the individuals whose data that is, when they weren't prepared. So, it's critically important to have that extensive discussion about cybersecurity, data security up front and if you can. Not always possible, but we always try to negotiate an audit right into the vendor contract, so that not only are you discussing the cybersecurity safeguards that you want in place, not only are you building them into the agreement, but you're also auditing to make sure that what the vendor says is happening is actually taking place.

[Kevin]: All right. The next category I want to talk to you about is indemnification, or who pays when something goes wrong. And this is really one of the most important provisions in any agreement before anything bad ever happens, you need to spell out who's going to pay, whether it's unauthorized access to or exfiltration of data that results in a breach, privacy litigation, violations of law, intellectual property claims, or even just claims arising out of the vendor's breach of the agreement itself. These issues need to be planned for and spelled out in the indemnification provision, and it's especially important to address these concepts when it comes to AI and biometric technologies, because we're seeing growing issues and litigation involving biometric privacy statutes, AI discrimination allegations, unauthorized data collection claims, and, of course, consumer privacy lawsuits. You want to anticipate all of these issues and potential claims before they happen and build out a fair allocation of the risk in your indemnification provision.

[Kevin]: It's like the old saying, an ounce of prevention is worth a pound of cure. So think about it. Plan for it, and transfer risk appropriately and fairly before it ever happens. Indemnification is critically important. The last issue I want to talk to you about is insurance. Why is this so important? Lots of people think it isn't. They think, well, as long as the vendors promise to defend me and indemnify me for anything bad that ever happens, I don't need to worry about whether the vendor has insurance. Well, here's the rub. An indemnification obligation is only valuable if the vendor actually can satisfy it financially, right? You can promise to defend and indemnify someone, but if you don't have the financial ability to do so, that promise is meaningless. That's where insurance comes in. It safeguards the vendor's indemnity obligation under your agreement. So how do we make this happen? First things first. We want to make sure that the vendor has in place the key types of insurance, first- and third-party cyber coverage, technology errors and omissions coverage, and general liability coverage.

[Kevin]: Next we want to make sure the vendor has these categories of insurance in the right limits. We've seen contracts with limits as low as $500,000. We see contracts with requiring limits of up to $5 million. $5 million may be too high, especially for an emerging AI vendor. $500,000 is too low. You want to look for limits of at least $1 million, and to be safe, you want it to be two. Why? Because, as we'll talk about in a moment, this insurance is not only to protect your vendor and to safeguard its financial obligation to you, it's going to protect you as well. So once you've satisfied yourself that the vendor has the right categories of insurance in the right limits, you want to understand, at least generally, what the insuring agreements are in those policies. Now when it comes to a GL policy, you're probably not going to have much doubt because general liability policies have had standard policy language for many, many years. Not so when it comes to cyber coverage and even technology errors and omissions coverage. So if you can

get those policy forms or at least a summary of the vendor's coverage, that's best practice. You also want to know whether there are any key exclusions. Now on in particular that I would be concerned about would be AI exclusions. Carriers are beginning to incorporate AI exclusions for claims arising out of or caused by the actual or alleged failure or misapplication of AI. You don't want one of those exclusions in the vendor's policies, because that exclusion will bar coverage for the vendor and for you. So you need to look at that carefully.

[Kevin]: Finally, you want to make sure that you are named as an additional insured on your vendor's policies, on a primary, non-contributory basis. What does that mean? That means if there's a loss and your vendor is required to defend and indemnify you, that your vendor's insurance pays before yours does. Very important, because if the loss you suffer is due to something your vendor did, that insurance should go first. And if and when it does, it's going to save you in the long run on your own insurance premiums.

[Kevin]: Before I forget, I want to add one more bonus provision to consider. And that is the dreaded auto renewal provision. Lots of vendor contracts provide in the fine print for auto renewal, if you fail to object or raise the issue. And that means you could be stuck in a contract that really should last only one year, for two or three or 10 years. You want to avoid that. You want to bargain for the right to terminate that contract within a reasonable period of time. It might be 15 days if you need that, it could be 30. Anything that avoids the dreaded auto renewal is something you should consider. So what did we talk about today? We talked about generally negotiating a contract. Do you start from scratch or work from the vendor's draft? And then we talked about what in my view are the key provisions: cybersecurity, indemnification, insurance, and yes, the dreaded auto renewal. If you focus carefully on these provisions, you read the fine print, and you approach negotiating with your vendor in the spirit of achieving a win-win compromise, negotiating vendor contracts can be a relative breeze, not literally a breeze, but a relative breeze.

[Kevin]: The point is it doesn't have to be a hard-fought negotiation. It doesn't have to be a battle. Vendors really do want to work with you, and most, in our experience, are willing to do so. It's just critically important that you see the red flags and risks in the vendor contract before they come up to bite you. That's our episode of *Cyber Sip*. I hope you've enjoyed this one. Hit me in the comments with any questions or experiences that you have, I'd love to hear about it. If you have ideas for future episodes. Love to hear about that as well. For now, thanks for joining us and we'll be back soon with another episode.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, and Spotify. Like, follow, share, and continue to listen.