Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 11: "10 Traps in Technology Contracts, With Charles Nerko"

Speakers: Kevin Szczepanski and Charles Nerko, Barclay Damon

[Kevin Szczepanski]: Hey, everyone, this is a Barclay Damon Live broadcast of Cyber Sip. Practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

[Kevin]: Hey, everyone, welcome back to Cyber Sip and we are so pleased to be joined today by Charles Nerko. Let me tell you a little bit about Charles. Charles is a graduate of both Fordham and Fordham University Law School. After law school, he clerked for Chief Judge Loretta Preska of the Southern District of New York. He was in private practice for many years, including as a principal in the Offit Kurman firm. And today Charles is a partner of Barclay Damon, where he practices and to name a few, the Commercial Litigation, and Financial Institutions practices. He is also the co-leader of the Barclay Damon Cybersecurity Team. We're happy to have Charles Nerko with us today. Welcome to Cyber Sip, Charles.

[Charles Nerko]: Thank you, Kevin. It's my pleasure to be here.

[Kevin]: And happy to have you. We've been planning it for a while. Glad to finally be able to sit down with you. Today we're going to talk about "10 Traps in Technology Contracts." Today, more than ever before, organizations are doing much of their work through outside vendors. So really, we're talking about traps in technology contracts with vendors. Let's just take a minute, Charles, and tell our audience about the different types of vendors that come into play.

[Charles]: Yeah, of course, thank you, Kevin. So every organization relies on critical business relationships with their technology providers in order to stay afloat. The technology powers the business, does day-to-day transactions, even for the most run-of-the-mill brick and mortar store. The technology powers the financial transactions, record-keeping, and on this podcast, we're going to talk about 10 ways to make sure that you maximize the value and reduce risk with those technology transactions that are so critical to business success.

[Kevin]: Right. So we're talking about traps in technology contracts, but I was thinking about this before we got on. I know we were chatting about it briefly. They are only traps if you sign the contract before you think them all through. Right?

[Charles]: So that's right. Is in my view, there is no such thing as boilerplate in a contract and even the most rudimentary provision could come back to haunt you later. So it's in terms of spotting the issues, how these could become traps, as well as how to mitigate against them. Some traps can be addressed in terms of the contract process. In terms of proposing alternative language, some traps are really a failure of the business to implement a process to just account for certain clauses, such as allowing a contract to auto renew just because the contract termination date wasn't placed in the calendar in a notice of non-renewal timely served. So we'll talk about all those ways to reduce those risks on the

legal as well as the business side.

[Kevin]: All right, let's get right to it and critical again to talk through each of these issues up front with the vendor with whom you're doing business to avoid the trap later on. So number one on our list is what you call the "entire agreement provision." How does that work? How can that be a trap for the unwary?

[Charles]: It pains me, it pains me when clients have a robust and diligent RFP process. They collect so much information on a vendor. And then when it comes time to sign the contract, they sign a contract with an entire agreement provision. And it basically says that once you sign the contract, the contract itself defines all of the vendor's rights and obligation, and that could cancel out everything the vendor tells you as part of the RFP process. So if there's critical information about the vendor you're relying on, make sure that's incorporated into the contract, and the contract reflects the reality of what the vendor is promising you.

[Kevin]: Yes. So, Charles, give us an example of the kind of information that can be lost in the context of an entire agreement provision that you might otherwise want to keep in the contract.

[Charles]: Sure. So, you know, as part of the vendor's marketing materials, you could be promised a certain level of security for certain service levels. And this goes into our number ten or number two issue, which is getting good performance standards and service level agreements. You want to make sure that everything the vendor promised you ends up in the contract. You want to have a clear allocation of responsibilities and clearly defined benchmarks to hold the vendor accountable and make sure that they're following through on their promises.

[Kevin]: So on that point, the performance standards, Charles, are sometimes we've had... worked with clients over the years where the vendor relationship will be perfectly fine. But then when it comes time to build some of those performance standards into the agreement, the vendor will hesitate. What does that tell you about the potential relationship going forward, when the vendor is reluctant to incorporate something important into the written document?

[Charles]: I think it's that the contract of a vendor is telling. It's a way to kick off the relationship. And usually clients don't look at their contract when things are going well. It's usually when things are going bad and there has to be good rules about what happens when things go south. So I think it's really telling that if a vendor as part of the RFP process promises you the world but isn't willing to put that commitment into writing as part of the contract.

[Kevin]: Yeah. All right. So number three on our list of top 10 traps in technology contracts is something that you call "exclusivity." Tell us about that, Charles. What does it mean and what should we be wary of?

[Charles]: Yeah. So I've been seeing increasingly seen vendors required exclusivity agreement as part of their technology contracts. And this makes sense at some level. You don't want a company coming in, providing technology, performing record-keeping services and have to deal with a competing vendor and trying to reconcile two vendors with proprietary data formats trying to harmonize with each other. So in large agreements a vendor will sometimes insist on exclusivity. I think it makes sense for the single service that you're looking to contract. What I've seen some vendors do is insist on exclusivity for what they call the entire subject matter of the technology agreement, which could also give a vendor essentially a veto over using other technology vendors in unrelated contexts. So I think there's a proper way to balance this clause to make sure that you're not inadvertently marrying yourself to one vendor for future unanticipated services that you may be needing in the future.

[Kevin]: So. Important to look for that up front. All right, so let's move now to the fourth potential trap in technology contracts, and that is something we've seen we both seen, and I know our co-team leader Nick DiCesare seen it. We're going to have him on in a future episode to talk about some of these things. And that is duration and early termination. How does that come up as a trap in vendor contracts?

[Charles]: Sure. What works today in technology doesn't necessarily work in the future. I've seen contracts as long as seven or even 10 years, which is an eternity when you deal with technology. I would also have companies be vigilant because sometimes adding new services results in extending the term of a technology contract, and you can actually have different contracts with the same vendor with non-coterminus contract dates. And some vendors like doing this to add confusion and complexity, and it makes it really difficult to exit the contract or even to know when that relationship ends.

[Kevin]: OK, so that sounds … Sorry to interrupt. That sounds really important. Let's break that down. So I'm thinking of this as "I've got a two year contract with a given vendor," but I decide midway through year two that I want to add a service. You're saying that by adding that service, I may unwittingly be extending the two-year term of my original contract.

[Charles]: That's correct, I've seen contracts do that. Just as an example, there is an interesting study done by Bank Director a couple of years ago—and banks are probably the most sophisticated when it comes to contracts. One in five banks didn't know when their core technology contract ended. And the way Bank Director conducted did this survey, it wasn't a trick question. It wasn't "does the contract expire at 5:00 p.m. or midnight." It's not even "does it expire on March 5th or 6th." There was only four possible answers to the survey and it was a) my contract expires this year and next year, b) my contract expires in the subsequent two years, c), my contract expires later than that, or d), I don't know.

[Kevin]: Yeah.

[Charles]: And one in five financial institutions couldn't even give that two-year band about when their contract expired. And that's because the contracts are confusing, long, and sometimes these little addendums can unwittingly adjust the contract date. So it's important to make sure before you sign anything, including a supplement or a new addendum, that you're making sure that it's not changing the date that you originally intended the contract to exist for.

[Kevin]: What I think is so important about that, as you say it, is that thinking about good cyber hygiene and organizations' IT needs, their information security needs, are constantly changing and evolving over time. And it just strikes me that if I as an organization don't know when my various technology contracts expire, it may suggest that I am not as on top of my technology situation, my information security safeguards, as I should be. So if you don't know when your contracts expire or you have an issue in that regard, it may be time to take a broader look at what services you're getting, from what vendors, and whether it may be time to revisit that.

[Charles]: Absolutely, Kevin. And a related concern I've seen, too, is not knowing when to send a notice of non-renewal. So a lot of contracts will automatically renew after a set period. Some vendors, you have to provide three months' notice, six months' notice, even a year notice before that contract doesn't begin for another cycle. And it's important as soon as you sign the contract to calendar that date. So you know when to sign that notice of non-renewal. I've had some clients even immediately after signing a contract, follow up the next day with the notice of non-renewal just to mitigate the risk of an inadvertent non-renewal, and keep that from automatically happening.

[Kevin]: Critically important. So that brings us to trap five in technology contracts, Charles: limited liability. A

critically important issue. Tell us about how that can raise issues in technology contracts.

[Charles]: Sure. So when you contract with a vendor, it's important to think about all the bad things a vendor can do to you and does the limitation of liability provision reflect a fair allocation of risk? For example, I've had one client that was a financial institution, and its vendor that was computing transactions had a computational error that resulted in thousands of consumer account statements being inaccurate, and the client faced two class action lawsuits from its customers based upon being charged fees because of the inaccurate records. What redress do you have against the vendor if there is a catastrophic event like that? Usually, most vendor contracts begin with a one-sided limitation of liability, saying that the vendor, if something goes wrong, won't be on the hook for that much. It's important to try to negotiate this provision so that there's a fair allocation of risk in case something goes wrong and you need to go back to your vendor to make sure they're there to make it right.

[Kevin]: Absolutely. I think a lot of times an organization will look at a technology contract, particularly those limited liability and warranty provisions, and assume that they're sacrosanct. But very often vendors are willing to negotiate those provisions, right? I've actually seen vendors become willing to negotiate a limited liability provision if you build into the agreements, a promise that the liability will be limited to the extent of available insurance. So the vendor knows it's going to be liable, but knows that there's essentially a cap on that liability. Have you seen that, Charles, and how do you find vendors to be willing to negotiate that provision?

[Charles]: Yeah, thanks Kevin, I think these clauses require a creative look. So typically, vendors won't accept liability for customer errors or customer-caused issues. When things are within the vendors control, you can carve out distinct liability caps or adjustments, as you suggested, such as limiting or allowing more liability if there is a bucket of insurance available, or increasing liability for certain acts or omissions of the vendor that's exclusively within the vendor's control and it's not something that could be caused by the customer.

[Kevin]: Yeah, that's why it's so important to have the conversation before you sign on the dotted line. All right. So number six, the sixth trap in technology contracts related to limited liability, and that is indemnity. Talk to us about what that is and how it can become a trap in technology contracts, Charles.

[Charles]: Sure. So indemnity essentially means that if you get sued because your vendor did something, you can bring your vendor into the lawsuit. They would have to defend the lawsuit and ultimately fund a settlement or an adverse judgment against you. I think our first Cyber Sip did a great treatment on indemnity for cybersecurity problems, and as we think about technology contracts, there are some related problems as well that also require a critical look at the indemnity provision. So, for instance, a lot of banks offer remote deposit capture, and that's that cool technology when you want to deposit a check, you can take your mobile device, take a photo of the check, and deposit it into your bank account. The bank that invented that is USAA, and they specialize in having bank branches on military bases, and they invented this technology in order to better serve service members across the globe. USAA has over 50 patents related to this technology. And if you're a financial institution that's doing remote deposit capture, there's a chance that you may infringe on one of these patents. And whether the technology infringes on that patent is really a technical issue from the vendor side. So in that context, we've asked vendors to provide an indemnity for patent infringement because how the technology works is really within the vendor's control and the ultimate end users of the technology shouldn't be assuming the business risk that the vendor may be infringing on a patent. So as Cyber Sip episode one said, for the indemnity provision, you want to make sure that you cover cybersecurity incidents and data breaches. And we would also add too that you should take a look at a patent and IP infringement indemnity as well and make sure that the vendor is accepting

accountability in case those issues arise.

[Kevin]: So you could always have that risk as an organization, but you want to make sure you do what you can to transfer that risk to the vendor, who is in the best position to be able to manage it.

[Charles]: Absolutely. This is, you know, vendors are usually proposing terms that don't mention unique things like cyber incidents or IP infringement. But when the customer raises it, vendors are usually willing to stand behind their service offerings and say, Yeah, we'll cover you for that because we understand that's a problem that's really in our control.

[Kevin]: Yeah, but a critical highlight of a serious potential trap, Charles, because very often we see indemnification provisions that just are not built for IP or cybersecurity. Got to make sure that that that indemnity provision really fits the nature of the relationship that you have. All right. So let's move on to the seventh trap in technology contracts, and that is dispute resolution. So you've got options when it comes to resolving the dispute that you never want to have. Right. And one of them is to simply go to court about it. But there may be alternative methods of dispute resolution, like mediation, arbitration, so how can this become a potential trap for an organization?

[Charles]: Sure, it's important to make sure that the dispute resolution clause allows a fair method of resolving disagreements with the vendors. Sometimes vendors propose terms that favor themselves. So, for instance, you'd be...if there's ever a dispute you, as the customer would be required to go to the vendor's location in order to sue them or have an arbitration proceeding. A lot of vendors will stick to this as part of their contracts, but it's important to be aware of what's actually required if there is a dispute. If there's an out-of-court dispute resolution process, make sure that that's fair for your organization. So, for instance, I've had clauses where the vendor will not allow discovery in private arbitration, which makes it a significant disadvantage to have a dispute resolution process that's successful. I've also seen vendors propose that the arbitration occur before a panel of essentially other users of the technology. And then you're essentially forced to litigate your claims against, you know, what, satisfied customers of the vendor adjudicating that. So whatever the vendor proposes, think about how it will work in practice and make sure that it's fair for your organization.

[Kevin]: So we're not saying that an alternative method—like arbitration—is necessarily the wrong method, but you want to make sure that whatever method is built into the contract gives you a fair opportunity to gather the evidence that you need to support your claims.

[Charles]: Right. An arbitration can be a fair process. So can litigation. It's just important to make sure that you see what else is involved in administering that process, and that if there's impediments to successfully presenting a case, that those are removed from the contract.

[Kevin]: You know, that's a great point. It reminds me to put a plug in for a future podcast episode. We're going to have Andrew Nadolna, the mediator arbitrator from JAMS, New York, come in and talk to us about the tips that he'd like to share about arbitrating business-to-business disputes in the cybersecurity realm. So we'll look forward to having Andrew on and maybe have you join him, Charles, we can have a wider discussion about ADR and cybersecurity.

[Charles]: That would be great.

[Kevin]: But for now, let's move on to the eighth potential trap in technology contracts, and that is something that you call deconversion or termination fees. What's that and how is it a potential trap for us?

[Charles]: As soon as you sign a vendor agreement, you want to start thinking about the end and what does

that prenup going to look like? You have to think about what's going to go on next, when I need to replace this vendor, or the vendor goes bankrupt or no longer exists. Do I own my data? How much does it cost to get my data back? Will the vendor provide assistance in transitioning your company's data to a successor vendor? And also too, if the relationship isn't working out? Is there a contract exit fee, which is called liquidated damages, for getting out of a bad deal? These costs can be significant and a lot of contracts the vendors will say that they'll provide a transition assistance at their standard rates. And I know from doing this that when you're trying to leave a vendor, the standard rates are pretty tough because they know you're on your way out and there's not an incentive to minimize those costs on the vendor's end. So the extent that it's possible, it's good to have a clear definition of what fees are going to be charged at the end of the relationship and make sure that they're fair and proportional to the services actually required to transition or end that relationship.

[Kevin]: Yes, that's great advice, Charles, I know it's difficult to plan the breakup at the outset of the relationship, but if you take some practical steps, you can make that breakup, which you want to avoid, but if it does happen, you can make it much more efficient and cost effective for your organization. That's a great trap to avoid. We're on now to the ninth potential trap in technology contracts, and that is data ownership. This one always surprises me that vendors would want to own data that is not theirs, but talk to us about how this comes up and what we should be mindful of.

[Charles]: Yeah. So the ownership of business records is critical for an organization. You want to own that data so you can use it freely. You can transfer it to a new vendor and you're not worried about a terminated vendor still maintaining your data after the relationship has soured, a terminated vendor in particular doesn't really have the business incentive to safeguard your data against evolving data breach risks. So in the contract, I would make sure that you own your data, your vendor is given access to the data to perform a service, and they shouldn't be owning your organization's data as part of providing a service. I've seen data ownership provisions get litigated before because some vendors like to assert that they own their customers data and at the end of the day, the customer's data should belong to the customer itself and not a vendor who is a limited service provider to an organization.

[Kevin]: Right, fair point. Very important. And that brings us to the 10th and by no means the least important trap in technology contracts, and that is the issue of audits, Charles. Tell us about that. I think you were kind enough to refer to our earlier podcast on "The Three Cs of Cybersecurity" for vendors. So the first C is confer and we're talking about traps that we should confer about before they become built into the contract. And the second C is the contract and the third C is comply. And that's the concept of the audit that we're talking about. So you can have all of these provisions built into your agreement. But what happens if you're not making sure that the vendor is actually fulfilling its promise to comply with those things?

[Charles]: Absolutely, Kevin, that's why the final C is so important, particularly when we talk about a multi-year contract. What's true today may not remain true for the remainder of the contract, particularly in the cybersecurity context, where threats evolve over time, and your organization wants to remain confident that the vendors continuing to do the right thing and make the necessary investments to protect against emerging cyber risks. So look at the audit provision in the contract. It should give your organization rights to make sure that the vendor is continuing to do what they promised at the outset of the relationship for the remainder of the contract.

[Kevin]: And I think you just made this point, Charles, but I want to underscore it because I think it's so important that an organization realize that it's not enough just to have the audit right. You want to use it for really two reasons. First, you want to make sure that your vendors doing the things that you agreed your vendor would do. But if something does go wrong and there is, heaven forbid, a cyber

incident or potential cybersecurity exposure, being able to look back and say, well, at least we took reasonable steps to audit our vendor and make sure that the vendor was doing what we wanted the vendor to do can be critically important in responding to an incident, especially when you're dealing with regulators.

[Charles]: Absolutely. Particularly for organizations that are in highly regulated industries such as financial services. I have some financial service clients that will actually perform an onsite audit and fly out their employees to a vendor's data farm just to make sure that the proper protocols are in place and that the documentation the vendor supplies is actually carried out in practice.

[Kevin]: Well, Charles, thank you so much for coming on to talk about 10 traps in technology contracts. I think this is really a template that every organization should have at the ready when negotiating its next vendor contract. I really appreciate you coming on.

[Charles]: Thanks, Kevin, it's my pleasure. Happy to be a resource.

[Kevin]: Well, thank you, Charles, and thanks to all of you for joining us. We'll be back soon with another episode of Cyber Sip.

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