Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 1: "Episode 1: Introduction"

Speaker: Kevin Szczepanski, 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.

[KS] Hey everyone, I'm Kevin Szczepanski. Welcome to the Cyber Sip podcast, and I want to make a special welcome to all of you to our very first episode. I'm very excited to be bringing it to you today. We're going to talk about the three Cs of cybersecurity for vendor relationships. But before we do, I thought you might like to know a little bit about why we're doing this podcast. Why is the BD cybersecurity team bringing you this podcast on Barclay Demon Live? And here's why.

It really goes back to when I first started in the cybersecurity realm several years ago. I was excited about it; I knew it was important, but I also knew that I had to catch up to learn all of the technical details that are so critical in this industry. So I grabbed a hold of everything I could find. I read every article online, I read every book I could find. I went to every conference I could attend. And yet I still found the barrier to entry to be challenging because it is, as I said, a highly specialized industry with some terrific IT and information security professionals. But there's a gap between the language that you and I might speak and the language that the experts speak. And so we thought, what better way to bridge that gap than to offer a podcast with practical tips in plain terms that everyone can understand and that everyone can use to embrace the mission of cybersecurity? So that's what we're doing. I hope you enjoy it as much as I'm enjoying bringing it to you.

And let me also say how we're going to do it. Some of our podcasts will be just me speaking to you about some topic of the day, some current event that we think is critically important for you to hear more about. But for the most part, we're going to bring in guests, industry thought leaders, to talk to you about everything from compliance to prevention; breach response; we're going to talk ransomware. We're going to talk about regulatory investigations, litigation, and yes, we're going to talk about cyber liability insurance as well. So we're excited about it. I hope you're excited about it. Let's turn now to the three Cs of cybersecurity for vendor relationships.

But first, a caveat. We are hoping to give you practical tips that you can take back to your organization to help improve cybersecurity and help you think about cybersecurity. But we know every organization is different; every situation is different. So the tips we're talking about today and in future podcasts may or may not apply directly to you. If you have questions about how our tips or how our discussion applies to your organization in particular, you can reach out to me or any one of our BD cybersecurity team co-leaders at BarclayDamon.com, and we can talk more about your specifics.

All right, so what are the three Cs of cybersecurity for vendor relationships? Let's list them and talk about each one. The first is "confer," the second is "contract" and the third is "comply." So the first "C" of cybersecurity for vendor relationships is confer. Very simple, but very important first step. You sit down with the vendor who is going to be performing services and you have a conversation about what data is going to be used. Who's going to have access to it? What's the scope of their access and what cybersecurity precautions will be in place? And as for what those precautions could be, they run the gamut. At one extreme, you might see a provision that simply requires the use of commercially reasonable safeguards.

But increasingly, we're seeing provisions that will obligate the vendor to comply with very specific requirements, including NST, ISO 27001 or if you are an organization that accepts payments by credit card, you may be required to comply with PCI (or payment card industry) standards.

So you've conferred and you're ready to proceed to the next step, the second C of cybersecurity for vendor relationships, and that is "contract," and that's where you build the protections for you and your organization right into your vendor agreement.

There are three important ones that I want to talk to you about. First is cybersecurity. The second is indemnification. And the third is insurance. Cybersecurity can be one of the most challenging to negotiate, but it's actually fairly straightforward. This is where you build the cybersecurity requirements that govern the agreement right into the contract, whether it's commercially reasonable safeguards or compliance with NST or SOC or ISO 27001. Whatever it is, you want to build that right into the language of the agreement.

Second, indemnification—now I'm sure many of us already have standard indemnification provisions built into our vendor agreements, but we've seen those provisions over the years, and in many cases, they do not extend to cybersecurity or cyber liability—most often govern bodily injury or property damage, sometimes breach of contract. The point is you want to review your indemnification provision to make sure that it includes liability for data breach, system breach, or other cyber incidents.

The third provision you want to make sure you build in is a provision for cyber liability insurance. You want to make sure that your vendor has that form of insurance and that you, as an organization working with your vendor, are named as an additional insured. That gives you an extra measure of protection. Because if something goes wrong, not only is your vendor required to make you whole, but your vendor has the insurance in place to pay for that indemnification. Critically important.

So you've conferred, you've contracted. And now we're at the third C of cyber security and that is "comply." You can have all the cybersecurity protections in the world, but if you're not taking steps to ensure that your vendor is actually following through, those protections will be worthless.

So. What do we mean by "comply"? You want to build audit rights into your agreement, and you want to follow up with your vendor to make sure—on a monthly or semiannual basis—that your vendor is actually following through on the cybersecurity protections that it's agreed to implement.

You want to make sure that your vendor is training its employees as well, particularly the employees that are going to be handling the data that's part of the agreement. Oftentimes, we build protections into a contract, but if they don't filter down to the people that are actually handling the data in the field, those protections don't help much.

So, the third C of cybersecurity, “comply,” ensures that what you contract for is actually getting done.

All right, so those are the three Cs of cybersecurity for vendor relationships: confer, contract, and comply. If you follow that roadmap, you’ll not only protect your business, but place yourself in the strongest position to defend your organization in case anything goes wrong.

I hope you’ve enjoyed this podcast. Thank you so much for listening to our first episode of the Cyber Sip. We’ll see you next time.

Disclaimer:

[KS] *Just so everyone knows, this material is for informational purposes only and does not constitute legal advice or a legal opinion, and no attorney-client relationship has been established or is implied. Thanks for listening.*