Barclay Damon Live Presents: The Cyber Sip Podcast™
Episode 27: "Don't Be the Weakest Link: Good Cyber Hygiene," With Brian Rice

Speakers: **Kevin Szczepanski**, Barclay Damon, and **Brian Rice**, Synapse LLC

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

[Kevin]: Welcome back. Brian Rice joins us again. For those of you that remember Brian from last time, he is the chief information technology officer for Synapse LLC, which is a specialized wholesale insurance broker with offices around the country. They're a good friend of the firm and Brian is a good friend of Cyber Sip. Welcome back.

[Brian]: Thanks for having me. Appreciate it.

[Kevin]: So when we were preparing for our first episode together, I saw this line on your website and it really drew me to it. It is "the ethical and legal ramifications of ineffective cyber defense postures." And basically what you're talking about is the ethical, legal, and moral obligation of every organization to protect customer data, employee data and business-sensitive data.

[Brian]: Absolutely. I mean, it doesn't matter if you're a yoga studio down the street. You know, it doesn't matter if you are $800 million, $800 billion company and everywhere in between, you have to protect your customer data because it's all based upon trust.

[Kevin]: Yeah. And if you don't, even if you're that small yoga studio, if you collect your customers' data, if you have what we call PII, personally identifiable information, which you're going to have if you're collecting payments by credit card, you do have you've got a legal duty to protect that information. If you don't, you're going to have the duty to provide notice and disclosure not only to the affected employees, but also to—depending on how many people have been affected by the data breach—the law enforcement, the attorney general of every state in which you do business. And for a lot of organizations are doing business all around the country. So there are legal obligations. But I think about my profession, Brian, is as lawyers, we have an ethical obligation to safeguard our client data as well. And it comes up in three ways. There's the ethical duty of competence. And a lot of lawyers don't appreciate that competence is not only familiarity with and facility in the subject matter of your representation. So for me, cybersecurity and my other life—insurance coverage, litigation—but also confidence in the technology that you're using to deliver services. So if you're talking on a video platform and you don't know what safeguards that platform has in place, or if you are communicating with a client by email or even telephone and you haven't disclosed to the client what the risks are in the use of certain technology, that's a potential issue. The other the other two ethical obligations, of course, are communication. So we have to be confident in the technology that we're using. We have to communicate with our clients about the benefits and risks of that technology. And third and most important, we have to safeguard the confidentiality of our client communications. So cybersecurity is really front and center when it comes to the ethical duties of a lawyer. So that's what I was thinking about when I read your line about the ethical and legal ramifications. Tell me what you were thinking about, because I know you're very passionate about this.

[Brian]: Everything you said is right on point. Everything you've already said is right on point. Everything that any company does has to have a moral obligation to protect your clients' data, whether it's PII—personally identifiable information—or PCI, personal company information. It's really critically important to make sure that everyone understands that they all have a moral obligation to protect their clients' data no matter what it is you do: yoga studio, law firm, $2 billion insurance company, it's irrelevant. This platform is the same. Mechanism is the same. You have to make sure that you're protecting your clients' data, because it's all based on trust.

[Kevin]: Yeah. And when it comes to legal, I touched on it earlier. There are not only legal obligations that arise from breach notification laws. So again, if a company suffers a data breach company is going to have to disclose, at least potentially going to have to disclose that breach to affected customers and employees and provide services including credit monitoring to those employees. And increasingly, Brian, we're seeing lawsuits brought by customers who learn that their data has been compromised, wasn't happening as much two years ago or even one year ago. But now just this year, I think we have our third or fourth class-action lawsuit brought by a customer who said, hey, I just learned that my data from ten years ago might have been compromised. I'm filing a class action lawsuit against your company. And then as a company, you have to pay for the lawyers to defend you in that lawsuit, which can go on for years. And if (we hope that certainly hope it doesn't happen), but if the customer prevails in that lawsuit and wins a judgment or negotiates a settlement, the company is going to have to pay that judgment or settlement. And sometimes there's insurance for it and sometimes there isn't. So that's one aspect of legal compliance. Another aspect, Brian, is the law of the contracts that an organization has with vendors. For example, so if I'm doing business with Synapse and I agree to—increasingly this happens—I agree as part of the contract that I'm going to be receiving certain data from you. I have a legal obligation under contract to protect that data. And if I don't protect that data, then Synapse could be responsible. I could be responsible. And I may face a claim from Synapse or whoever's data I was supposed to protect for failing to do so. So these legal obligations come from many different directions, and it just points up your point about maintaining this ethical obligation to protect client data.

[Brian]: Well, I mean, honestly, like, it's all supply chain, you know, like one company does business with one company, does business with ten other companies. And so every single person has to be responsible in their own company's organization to make sure that they maintain the integrity of client data across the board. And so... Synapse Partners, like what we've been doing across the board is making sure we set up questionnaires, every single person that we do business with as a obligate themselves to a questionnaire of cybersecurity and cyber compliance. Obviously, the insurance business, as you know, is very complicated. There's so many mechanisms that they're responsible to, no matter which state you're operating in. But take the same see the same scenario, apply it to a yoga studio. If someone gets into that business's, you know, just contact history... supply chain hack is there immediately available because that one person who is a CEO of a multinational company is attached to the yoga studio. Same thing with a person who is only a paralegal at a small company, or just a cash register, you know, mechanism at a small Albertsons or whatever. It doesn't really make a difference because it's all supply chain. If they can get into one mechanism of one business, they have access to every single other person. And when they see the supply chain aspects of all of that, everyone is vulnerable. Everyone is culpable also equally.

[Kevin]: Right. And we saw that in the case of the Target data breach many years ago, the threat actor did not hack into Target itself. It hacked into an HVAC supplier to Target and from there was able to hack into the POS or point of service data that Target maintained for its employee transactions. So what you're saying is exactly right. So you may think that all that's happening is a data breach of a yoga studio, but if there is a customer of that studio who works for another business and the threat actor is able to get credentials for that customer and use those credentials to create a spear phishing or a targeted attack on that customer, then all of a sudden the threat actor gets... has access to the yoga studio, may have access to the customer's business and the tentacles of that hack spread out across multiple businesses.

[Brian]: 100%. Across the board.
[Kevin]: So I know we've got our time is coming to a close, but if someone were to come to you and say, okay, Brian, I get it, there is a legal, ethical, moral obligation and maybe there is a an economic motive as well to protect customer data, because I'm going to stay in business and I'm going to be able to distinguish myself from my competitors who may not be as strong in the area of cyber hygiene as I am. But let's say someone comes to you and says, okay, I know all of that. I get all of that. What can I do right now to improve my security posture so that I can minimize my exposure to these ethical, legal, and moral risks?

[Brian]: It's a fantastic question, Kevin, and I'll give you four main points. And most of them are all cheap, if not free. We mentioned KnowBe4: Absolutely every single person in your organization, no matter who you are, yoga studio or multinational company, has to have employee education and training on how to spot phishing. Number one. Number two, absolutely, institute a "this is outside of my organization's email" policy on Office 365 and G Suite. The two main company organisms for email free. Attach it because if somebody comes in saying they're the CEO of the company saying I need X, Y and Z. However it comes across as "this email came from outside your organization," you know, immediately. Immediately. This is false.

[Kevin]: It's fake. Right.

[Brian]: Exactly. That's number two. Number three, you absolutely have to have multi-factor authentication.

[Kevin]: All right. So let's stop there. Everybody thinks they know what multi-factor authentication is, but half of the people who think they know, they don't know. So talk to us about what it is and why it's important.

[Brian]: All right. Fantastic question, Kevin, again. And so multi-factor authentication, everyone knows that you... if you sign into your bank in a text message, you know, with a six-digit code or something of a sort. That effectively is a form of multi-factor authentication. Okay. So we all know what that is. And so, for your organization for Office 365 and or G Suite, you know, multi-factor authentication just means: it's multi-factor authentication. So you sign with a password the you prompted for a secondary means of authentication.

[Kevin]: A PIN or some sort of code...

[Brian]: Exactly. And so if you have like Duo or Okta, there's an actual application on your phone that can prompt you like, hey, someone's logging into your account. Is it you? Yes, I accept. Or No, it's not me. I deny. Okay. So there's also secondary companies that do that. But again, with Office 365, it's free.

[Kevin]: It's there. And you just want to make sure that you enable it.

[Brian]: Everyone has to have that as a check mark for doing business going forward. You absolutely have to have it. And number four, again, coming right back to the first point, employee training. The weakest link, always. 95% of all incidents and breaches come down to a personal deficiency of education and training. So if you're trained, and you know what to do and you have some basic free mechanisms in place, they're going to move on to the next.

[Kevin]: They're going move on to the next victim. And that training can come in many forms. You mentioned in our first episode together, we mentioned KnowBe4 and again, shout out to KnowBe4. We at Barclay Damon use it, it's K-N-O-W-B-E, the number four, dot com (https://www.knowbe4.com/) and that is an outside vendor that has an outstanding training program. I just completed my KnowBe4 training for Barclay Damon, it was supposed to take 45 minutes, it took me closer to 30 minutes. And frankly, I felt better afterwards that I was more capable of recognizing the increasingly sophisticated attack strategies that a threat actor will use. I know that if I'm getting an email from a potential client and it looks like legitimate business, but the email is from a Gmail account. I know legit businesses have their own email domains.

They don't email me from a Gmail account. If the greeting isn't "Dear Kevin" but "Dear Counselor" or... and it uses odd language or there are spelling errors throughout the email. This is the kind of training that you want to make sure your employees bone up on throughout the year. And having an outside vendor do it is really a smart move. But you can also train in-house, I think, Brian, it's a combination really, right? It's not just KnowBe4, but periodic training from within your organization, from someone like you, as the chief IT officer.

[Brian]: Sure. Absolutely. Anything that can get ...that can get very convoluted very fast also.

[Kevin]: Yes.

[Brian]: So you take the basic training for sure. Then you have to, you know, if you go through the whale phishing or spear phishing or social engineering or reverse social engineering.... it can get convoluted very, very fast.

[Kevin]: Right.

[Brian]: Right. But ultimately, if you're just doing the basic mechanisms, again, multi-factor authentication, external awareness training, and the other two that we talked about, as a matter of course, you're going to be covered most of the time. Again, however, it's important to note that it's not a matter of if, it's just when.

[Kevin]: When. Right. There, there are two kinds of companies out there, those that have been hacked, and those that have been hacked and know they've been hacked. So you're not going to prevent an attack entirely. What you're going to do is make it harder and therefore less and less likely. And you're going to make it easier for your organization to recover and transfer the risk of an attack, because if you have these security controls in place, including employee training, you're more likely in this very tight insurance market to be able to purchase cyber insurance. Which is getting harder and harder to come by.

[Brian]: 100%. And again, the mechanisms of the cyber liability insurance, social engineering, fidelity, everything across the board, it's all coming out of the same basic things. Do you have the same base mechanisms of protection for your organization going forward? And that's it...

[Kevin]: Yeah, that's right.

[Brian]: Yes.

[Kevin]: And I look forward to having you, and your colleague Demi is going to come on in the next couple of months and talk to us about insurance. I think that's a great place to leave it. Brian, I love this topic. Ethical and legal ramifications of ineffective cyber hygiene, something we all need to keep in mind because there are very real consequences.

[Brian]: Absolutely. And Kevin, thank you so much for allowing me to be a part of your Cyber Sip series. Anything I can do to help promote the education for everyone, for the masses. I'm here for 100% all the time.

[Kevin]: I appreciate it. You are one of the great ones out there, a true cyber evangelist. And I appreciate your coming on, Brian. Thanks, man.

[Brian]: Thanks, brother...

[Kevin]: All right. And thanks to all of you for joining us on this episode of *Cyber Sip*. We're back soon with another episode.

[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.

Disclaimers:

This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied. Thanks for listening.

Barclay Damon Live podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of Barclay Damon Live programming is the audio file.