Barclay Damon Live Presents: The Cyber Sip Podcast™
Episode 26: "Control, Test, and Train: Best Advice From 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, everyone. I am so excited to have Brian Rice join us. Brian has 20 years in the enterprise IT environments arena, and he is, today, the chief information technology officer for Synapse LLC, which is a specialty wholesale insurance broker with offices around the country. Brian, thanks for coming on, man, it's been a long time coming.

[Brian]: Absolutely, brother. Kevin, thank you so much for bringing me into Cyber Sip. I'm super happy to be here with you.

[Kevin]: Oh yeah. No, I am happy to have you. So before we get started, tell us where you were and how you found your way to startups to become chief IT officer.

[Brian]: Sure. Absolutely. I mean, so to make it a small and encapsulating conversation, I spent 20 years basically building up companies, making sure they're secure from a cyber defense, cyber... a smart cyber posturing standpoint for every single company that I dealt with, whether it be small, seven-person Manhattan law firm or a 700-person ABCD company, that's global, effectively. And building all those companies up to make sure that they're secure for every single person, for every single aspect of their business. I moved into a client, a longtime client, which is Synapse Partners, about three months ago, but they're a client of mine for seven years and building up from 33 people to now 120 people. That's kind of how I got there. It's a long conversation of how I got there, but most importantly, it's a matter of cyber defense, cyber security—the legal ramifications of what is and what can be a liability.

[Kevin]: Right. It's interesting you mentioned the growth in the company because we're going to talk a little bit later about the importance of employee training. But let's dive right in. So, I mean, there are a number of security controls out there. We just had a Cybersecurity Awareness Month in October, and we know that we: have to update our software. We have to have strong passwords, we have to have multi-factor authentication or MFA and a host of others like... endpoint detection and response encryption of data. But if you're a new organization or an organization that's new to cybersecurity hygiene, how do you know what controls you need to have in place and what may be something to aim for but isn't necessary at this early stage?

[Brian]: So it's a great question, and I would say that no matter what, you have to start your business off. You have accounting, you have marketing, you have sales, business development, you have cybersecurity. For me, cyber security goes first across all those boards. You have to have strong policies for passwords. You have to have MFA. You have to have encryption for all your devices. Doesn't matter what industry you're in, it really does not matter because the low-hanging fruit, 53% of all hacks, of all incidents, of all breaches, of all everything are small businesses. Why? Because they do not have the internal controls mechanisms to protect that company's data. So...

[Kevin]: And that can be a sad story, too—is if you're a small business and you suffer a hack or a data breach, your business is in jeopardy, right?

[Brian]: You're done. Right 100%. And that's why. And you have to understand that the hackers, the people that are the bad actors inside this is not basically the kid next door. Well, yes, it is, but mostly it's state-sponsored activity. So you have China, you have North Korea, you have Russia, you have all these people that are actually activating mechanisms to go and breach businesses as a matter of course. And so you have to understand that they have a level one, level two, level three supports of how to get into your business and go all the way through it. So if you're starting a brand new business, if you don't recognize the fact that you have to start your business with the most strong cyber posturing that you possibly can have from a defense mechanism, then you're automatically behind, effectively behind the great, you know...

[Kevin]: Yeah. And behind your competitors as well. Now one thing I hear—and it's not going away is...we did such an effective job encouraging companies to purchase cyber insurance that many of them will say, well, you know, I really don't need to worry about my cyber hygiene or having these controls in place, because if something goes wrong, I've got insurance, the insurance company will pay for it. What's wrong with that?

[Brian]: Well, that's definitely a conversation for getting my counterparts on the insurance side. However, I would say that no matter what your policy is, it doesn't change the fact that if you don't have all these controls in place, it doesn't make a difference. You can have a policy all day long, you know, like you can have a car insurance policy. But if your brake lights are out, you know, and you get rear ended, that's your fault.

[Kevin]: Mm hmm.

[Brian]: Also, policies...you can cover a bad mechanism on your own party.

[Kevin]: Right? And in fact, many policies. You're absolutely right, Brian. Many policies will exclude or limit coverage for risks that either you didn't tell the carrier about before the policy went into effect or you didn't have in place during the policy period. So, no, that's a great point. So we talked about some of the processes and cyber controls that need to be in place, like patching updates and strong passwords, MFA and encryption. Let's turn to testing, Brian. Talk to us about the importance of testing an organization's computer system and what that process looks like.

[Brian]: So great question, Kevin. And so internal and external testing are very different animals. You have to have I would say a very strong partner. That's actually... it's your company to make sure that you're testing internally and externally. So whether you're seven people at a company or 700 people in the company doesn't really matter to me, from my perspective as a defense expert. You have to make sure that you have a third-party company that is testing every single thing all the time, internally and externally. Now, the real question here is where... where does the vulnerability going to really come from? That vulnerability comes from almost always an internal person. 95% of all breaches are all based upon human error. So you can test externally all day long. You can have pen tests, you can have effective like massive $100,000 security systems on your organization. That's can tell you like two pieces of information where there are holes in your cyber defense platform, your perimeter, effectively. But you have to understand that most people aren't most people that are trying to get into an organization, they're not looking at your firewall external vulnerabilities. They're looking at internal vulnerabilities.

[Kevin]: Right. You're talking about the employees.

[Brian]: Yes.

[Kevin]: I think a lot of people missed that point. And I heard this described very effectively the other day. It's essentially the threat actors, the hackers out there...they've tried to hack into organizations' computer

systems. And to a great degree, we've done a good job of putting up those firewalls. So what the hackers have said is, well, you know what, I don't need to break in to the network, if I can fool an employee into opening the door and letting me in. Right.

[Brian]: 100%. Kevin, you're right on point with that, because that is the most ...that's the largest vulnerability for everyone. It's the low-hanging fruits is that if I can convince someone to type in their passwords, their credentials to a browser listing Microsoft's or listing Amazon or looks like, you know, PowerPoints or anything else of, of the course. That is how they get in 95% of all breaches and all incidences are all human error and that, social engineering, is the biggest key.

[Kevin]: So when we're talking about how best to train employees, whether it's a seven-person law firm or a 700-person organization, Brian, what's your best advice to businesses out there that are coming to you and they're asking, all right, so how do I train my employees to avoid phishing or spear phishing or other potential attacks?

[Brian]: So a great application is KnowBe4.

[Kevin]: Yes.

[Brian]: Any kind of security awareness training is the critical key to everyone's success because, again, Kevin, to your point, the lowest hanging fruits, the one person who's not paying attention is how they get into the door every single time. Maybe they apply pressure constantly or there's you know, there's a social engineering hack. Hasn't changed the fact that if you have knowledgeable employees where 95% of all breaches in all incidences basically occur because of an employee typing in information, they shouldn't be typing into an email with the right knowledge they can mitigate their own risk.

[Kevin]: Right.

[Brian]: Effectively, Kevin, 100% hands down. Your biggest key defense is training every single person.

[Kevin]: Right. So and a shout-out. I'm glad you mentioned that, Brian. Shout out to KnowBe4. If any of our viewers or listeners aren't familiar with it, we hear at Barclay Damon use it for our internal training. It's Know, K-N-O-W-B-E the number four dot com. (https://www.knowbe4.com/) Their platform is one of the best I've ever seen. And essentially it's going to train your employees to recognize social engineering fraud and essentially it's a zero-tolerance approach, which means unless you are convinced that it's a legit email, for example, you should assume that every email you receive is potentially fraudulent. And if that sounds difficult or impractical, it's really not. Because what training is going to teach you is how to recognize everything from the email address to suspicious links, to suspicious attachments to misspellings in a document. Whether an email creates a false sense of urgency, like you've missed a payment, or your financial information has been compromised. If you train your employees on an annual basis on how to spot those attacks, your employees become not only your first and last line of defense, but your best line of defense.

[Brian]: Absolutely. I mean, Kevin, you couldn't have said it better; effectively your employees are your weakest link, but also your best defense. Right. Train them no matter who it is. Just look at emails. Pay attention to the fact that maybe this questionable, maybe suspect. If they have that knowledge, then your business is better across the board by having them all trained.

[Kevin]: Right. So Brian, we've covered a lot of territory in a short period of time, from security controls to testing to employee training. And we're almost out of time. I wanted to talk with you about something in your bio on the Synapse LLC website. It is something you call "the ethical and legal ramifications of ineffective cyber defense," and I am fascinated by that topic. Would you come back some time and talk with me about that?

[Brian]: I would love to. I would bring in like your expertise, Kevin, with regards to the effectively... the laws that really correlates in to how you protect yourself. Because again, there's a legal, moral, and ethical obligation for every single company to protect their clients' data. And the biggest thing that everyone has to understand, it's all about trust. It is all about trust. And the way I correlate trust into the conversation is, it's like credit. It takes years and years and years to build up credit and it can be destroyed overnight. Same thing with your reputation as a business. If you don't put the cyber defense mechanisms in place, that trust is eroded overnight, and you can never gain it back. Ever.

[Kevin]: Right. Boy, Brian, that's a great way to think about it. And I think that's a great place to end. I look forward to having you back on another episode. Thank you so much for joining us today. I really appreciate it.

[Brian]: Looking forward to. Kevin, thank you so much for allowing me to be a part of your Cyber Sip series.

[Kevin]: It's my pleasure, man. All right. Well, thank you, Brian Rice, and thanks to all of you for joining us for this episode. We're back soon with another one.

[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.