Barclay Damon Live Presents *Cyber Sip™*
Episode 29: “Cyber Wellness: Tips to Keep Your Business Safe,” With Bill Haber

Speakers: **Kevin Szczepanski,** Barclay Damon,
and **Bill Haber,** TEKRiSQ

[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]: Hey everyone, we’re back with another episode of *Cyber Sip*. And this morning, very excited to have with us Bill Haber, the co-founder of TEKRiSQ. Bill, welcome to *Cyber Sip*.

[Bill]: Thanks, Kevin. Great to be here.

[Kevin]: Now, I know that TEKRiSQ believes very strongly in identifying a... or an organization’s true technology risk before taking any steps to remediate and reduce that risk. But before we get started, I want to ask you how you got started in the world of cybersecurity and why your experience led you to found TEKRiSQ.

[Bill]: Sure. That’s a great question. And I’ve had a long technology career in software companies, data platforms, cybersecurity solutions, medical devices, and...let’s say lots of areas dealing with sensitive data. And my co-founder, Dean Mechlowitz, with a similar background, he’s been in more engineering and pure cybersecurity types of companies. But our skillsets complement each other. I had an opportunity to work with and help found a wholesale brokerage years ago, focused on technology-oriented risk. And when I looked at the way that data was being collected, let’s... rather than data; the way people are populating applications, the way clients are interacting with the... with insurance carriers and their agents, I saw a lot missing. And I certainly saw an absence of true “diagnosis.” So, you know, root cause—what’s going on in this organization? What’s their cyber maturity? Do they practice, let’s say, “cyber wellness,” you know, their solutions in place, policies, procedures. I just found it very loosey-goosey and realized, you know, this is an extraordinary moment in time when people go to get insured and it’s an opportunity to really evaluate where they’re at and recommend things that will make them more resilient and get a real good look under the hood what’s going on its own organization. And that’s a missed opportunity; it still is for many reasons. So we sought to find a way to streamline that in fast, affordable ways that can help insurance professionals to get that proper view and, you know, really have a better way to prevent bigger problems down the road.

[Kevin]: It almost sounds like what you’re saying is that you had seen a situation where patients were going into the doctor’s office and the doctor was prescribing the antibiotic or the antiviral without first diagnosing the patient. So what you’re talking about, it seems to me, is, you know, we’ve got to get in there and we’ve got to diagnose the patient first. What are the risks to this organization of technology or data? And then based on those actual risks, we’re going to devise a solution that enables the company to manage the risk, to get insured, and so on. Is that that where you’re coming from?

[Bill]: Well said, Kevin. And yes, we deliberately use the “cyber wellness” term and I use that in some organizations that I participate and discussing these topics as well. But it’s very easy for people to understand. You know, driving wellness keeps you out of the doctor’s office. Proactive analysis of what’s going on is what helps you to correct problems before they become bigger. In fact, cybersecurity companies, when they look to deliver solutions to their clients, they prefer to perform risk assessments to identify where people at on the maturity continuum. What are they doing right? What are some clear gaps and how do we fill them? And, you know, there's a lot of companies that make full-time careers out of that. You can really, with focused conversations, using these principles, get the bottom of that pretty quickly. And that's really where we're focused—that checkup has to happen.

[Kevin]: And you're focused primarily on small- and medium-sized businesses. Why is that? Is there a need you see that isn't being met? Or is there some other reason?

[Bill]: No. You bet there's a need. That segment...we consider them underserved. Most of the focus of cybersecurity companies today are on the "haves." And when we say "haves," you know there's a digital divide with the haves, with CISOs and solutions and policies and procedures and well documented and in the "have nots," who sometimes don't even know where to get started. And so there's an opportunity to quickly engage those folks and have cybersecurity experts participate in conversations to analyze what's going on here. Where do they need help? Are these folks aware, are they driving wellness or are they lost and need help? And provide the recommendations to help them get there. So, you know, we saw a huge unmet demand and we're seeing a good cyber risk profile being critical to doing business today, almost as important as a credit report on Dun & Bradstreet. And that's part of the reason why cyber insurance is exploding. If we can help people to, you know, button up procedures and tighten their security stack, they're not necessarily that far away from being insurable. They just need a little bit of help.

[Kevin]: All right. So let's say I'm one of those have nots. I know that data privacy and security is important. I know cyber hygiene is important, but I don't know how to get there. So I'm talking to you. What's the first step that you take in order to identify and diagnose my cyber hygiene?

[Bill]: Sure, great question. So we believe the best way to do that is to start objectively with a technology risk assessment, looking at potential vulnerabilities. We have a few different ways that we do that, but we have a basic risk assessment that we deliver to most of our clients that's not more than 30 minutes. It's an online conversation that's fast, easy, and affordable. We strip technology jargon out of it. Then when we talk to people, we seek to understand how are you using technology? What are the things you use? How do you share data? Where does the data live? Who's accessing it? What methods do you use to secure it? And we used [garbled] principles to kind of dig into that. We also use a little bit of psychology and adult learning theory to arrive at some conclusions and make some recommendations.

[Kevin]: Tell me about that. Got it. I'm sorry to interrupt, but tell me about that. How does that that psychology and adult learning theory play into the analysis?

[Bill]: Sure. So sometimes the way people answer questions indicates a bit of uncertainty or there's a vague response and we find a way to come back to that and ask the question a different way to determine if we see an inconsistency or just evaluate with the confidence level that people have in their responses. That's really important. We see a lot of small business leaders believe in common myths, and we hear them every day when we talk to clients. Things like, Oh, well, I have everything in the cloud, so I'm good. Or but we use Macs exclusively here and Macs can't be infected with anything, right?

[Kevin]: Can we try it? I'm going to...I'm going to be pretty much who I am. And we're on a phone call. And you're working through the questionnaire, if you will, to sort of get a sense of my cyber hygiene and where I sit as an organization. So go ahead.

[Bill]: Sure. So, Kevin, do you have any particular ways that you secure your endpoints in the company?

[Kevin]: I think so, but I'd have to talk to my IT person. I'm not really sure how we do that.

[Bill]: That's fine. Do you have an idea of solutions you use or any tools you have in place that might be on your machine that's secure?

[Kevin]: Gosh. Well, first, I mean, what what's an endpoint?

[Bill]: Very good question. And I'll stop right there, Kevin, and explain. Right now, we know that there's confusion and there are far too many misrepresentations, omissions, concealment of facts, and incorrect statements that find their way into insurance applications. We know right away, through that simple exchange that the terminology may be confusing to you and it may not be something you're capable of answering. That's an important thing to understand. We want to make sure that we get that right before proceeding with looking for insurance or validating that you have certain controls in place when you really may not.

[Kevin]: Right. And I assume part of that is making sure that on that first call, because time is so valuable, you've got all the right people there. You're not just talking to the head of IT or the CEO. You want to have all the expertise on the call so that those questions can be answered.

[Bill]: Yeah. We usually ask for an individual to be nominated by the business leader who's most familiar with the use of technology. And we say it that way because, first of all, a lot of small- and medium-sized businesses outsource IT and some of the folks they outsource IT to may not have cybersecurity expertise. That's another one of the myths I was referring to earlier, that the IT guy must have everything in place. Certainly not true, and probably unfair to expect the IT folks to do it all. So we seek to understand who knows what's in place and who can speak to the tech stack. And that is oftentimes an IT person or an outside IT person. But sometimes it's a chief operations officer who's got better visibility of that than anybody else.

[Kevin]: So we're talking about this now in the context of insurance. So I'm a business that's come to you. I know from a vendor that I'm doing business with they need me to have cyber insurance in place or else they're going to do business with someone else. So I've come to you. I want to talk about insurance now, Bill. But first, let me ask you a question. Some might be thinking, why TEKRiSQ? Why can't I get to the same place by just calling my insurance broker and having my insurance broker walk me through the insurance application, completing… check the boxes; yes or no, answering the questions. Why do I need this extra layer (if it is really an extra layer? I think we both know it's not), but if I'm a business, I'm thinking time is money. I don't have time or resources to do this. Why do I need to add TEKRiSQ into the mix?

[Bill]: Excellent question. And there's a few reasons. Number one, the industry is trying to make the insurance agent also carry the responsibility of becoming a full-time cybersecurity expert. That in itself is dangerous. First of all, even full-time cybersecurity professionals have a hard time keeping up with this change. Second, insurance folks can't devote their career to getting on top of this. And you know, they can't go spend a weekend somewhere and get a certificate and call themselves an expert. And thirdly, there's a, you know, risk in playing that role and diagnosing risk on behalf of the client. What is critical is having cybersecurity expertise, folks who are knowledgeable and do carry certifications in various areas and can diagnose risk to take an independent, objective look. That independence, we think, is really important in the industry because we don't have a vested interest in the outcome. We're not interested in selling anybody insurance. We're making sure that the client builds enough resilience to become insurable. And then oftentimes we're in the process of certifying that those things are in place so the insurance process can move forward. The reason you might want to do that is not only is it helpful to have experts put their eyes on this, but in our case we try and do that in a fast, easy, and affordable way with very little friction, strip the technology jargon out of it, and we produce documentation that's easy to understand. It doesn't require them to know what "endpoint detection response" is, but makes them understand, you have to make sure the following types of equipment in use in your business are secured from chaos. If you want your clients to continue to work with you and entrust their data with you.

[Kevin]: Right. So let me ask you this, Bill. At what point do you come into the process? I'm guessing our audience members are thinking, okay, so there's an organization out there that can help me identify and evaluate my cybersecurity risk, and that may help me in the insurance process. Where do you come in? Do you come in at the time that the business receives the application to be completed? Do you come in before that? Do you come in after the company has been denied coverage to evaluate what steps need to be taken to maybe get coverage down the road? How does it work?

[Bill]: So we are often brought in in all of those different scenarios. But ideally, the way to do this is proactively. Before—well before—any insurance applications submitted. And that's part of the value that we provide. Having, conducting...having conducted an assessment, being able to populate market apps for them. That's a big part of the value of what we do. But it's also important because you want to make sure you get the responses right. The way we're brought in is typically through insurance agency relationships that we have. So we build relationships with agents who say, okay, I've got X number of renewals coming up and I'd like to start inviting my clients, you know, 60 days out to having this conversation and let's get it scheduled. We'll have that and all the value will flow from there. So ideally we're brought in by agents and increasingly we're working with carriers because we're getting endorsements filed and things like that, but brought in by agents, schedule the conversation with their client, conduct it quickly. And then we generate a lot of reports that recommend what they need to do to become insurable, to get the most attractive terms. And we can even propose those solutions. A lot of times the insurance agents go, all right, they need these things. Where do I go? We understand the top ten solutions that underwriters like to see in place, and we can not only deploy them, but this is where we use things like adult learning theory to help people, to adopt them very quickly. And we use some strategies to help them put them in place and quickly build a cyber culture and reward the people who move quickly. I ...kind of put their thumb on the folks who are lagging and become very responsible organization.

[Kevin]: So I know we're running out of time, but I want to ask you a couple of questions. One is related to what we talked about earlier, the sort of prescribing a remedy for the patient without first doing the diagnosis. There's so much out there today, and I think a lot of us think, boy, if you do nothing else, if you know nothing else, then at least enable multifactor authentication, at least have strong passwords, at least, you know, go through the cyber liability insurance underwriting process. And as I'm sitting here now, I'm thinking a lot of businesses must be thinking when they hear that, well, it sounds like you know what you're talking about, but I don't understand what any of that means. And until I do, I'm not going to focus on implementing what you tell me to implement. What's your thought on that, Bill? I feel like there are a lot of recommendations out there. They're all very valuable and generally they're critical. No one would argue that you don't need MFA, but with respect to what's trending these days, which is just sort of tell people these are the five things you need to do, without actually going through, looking under the hood and diagnosing the problem before you propose a solution. What do you make of that?

[Bill]: So we think employee complacency is the big problem. Most small- and medium-sized businesses are going to have cyber problems at some point, and they're not going to be nation-state attacks. They may not be enormous ransomware cases, but they're probably social deception, business email compromise, or someone convincing a human to do something stupid and compromise their credentials. So we think it's really important to get control of your credentials. And usually the place you want to start is becoming aware. Well, how do people do that? So we like to see that people put a security awareness program in place that not only gives them some fast, easy training to open their eyes to some of these things and test them a little bit, and we'd like to see the cadence of that monthly rather than, you know, one time a year.

[Kevin]: Right.

[Bill]: We like to see doing some phishing and trying to show them that this is how people are grabbing your credentials. And you need to be wary of these things. You need to know how to read your email. Those are some basics that are really good to put in place so that you can then start to do things like filtering mail. There's so much, you know, tricky messaging coming through the Internet, through email. We like to see things like DNS filtering. So all of the new sites that are that the hackers are spinning up quickly get just eliminated from being able to communicate with you. And depending upon what the nature of their business is, we might recommend a few different things. But everybody needs to be delivering training. Everybody needs to be aware of how they're...how the attack vectors are coming into their company. And typically, a lot of that is through email. And then beyond that, certainly putting endpoint protection and response like we talked in place and there's a handful of other things that can be industry-specific, but we look at where people have vulnerabilities and then recommend solutions. Too many cybersecurity companies that blanket them with a lot of things that become extremely expensive, unaffordable, and they're not pragmatic and they end up causing people not to do anything. And inaction is really the biggest problem.

[Kevin]: Yeah, super helpful. And folks, if you're listening to this right now, when you ask a cybersecurity expert to tell you off the top of his or her head, what are the three or four things you need to do right now? Hear what they say. Because very often it reflects the trend; where things are going and what the legal standard is, so that if you do have those things in place, you can not only prevent attacks, but you have the strongest arguments for a regulator or a plaintiff in a lawsuit to say, hey, I know this bad thing happened, but I did everything I could. I did everything reasonable to prevent it. Now I'm tempted to leave it there because I know we're running short on time, but I'm a lawyer. We can never leave it there. We always have to talk more. And I think you might have answered this to some degree, but I want to ask you anyway, so a thought experiment, Bill: you are going away for a year. You are getting an all-expense paid vacation to the most beautiful site in the world for you, but you're going to be completely out of commission. You're not going to be able to talk to a single customer. You're not going to be able to talk to Dean. And you're a little worried about this because you care about what you do. So before you leave for a year, so you're not coming back until January 2024, if you had to say one thing to a customer out there that's only going to hear you once, what would you say to that customer or that business about what they should be doing over the next 12 months?

[Bill]: Well, that's a great question. I mean, personally, I park my email, I'd suspend my email account and I do that because so many different things end up finding their way into your inbox or email. But aside from that, you know, I think if you know for a year that you're not going to have a need to access anything. And I think you're talking about a really small slice of humans, but, you know, I would suspend all of my technology access accounts, so not just email. I'd look at, you know, my phone, my Internet accounts, I'd go completely offline. I think that too many people put a lot of concern on keeping everything and being able...not missing anything. You know, the people that need to talk to you...they'll find you. No problem. That's easy to do in this world, right? You're not needing to conduct business and not needing to have regular exchange with people. Shut it down.

[Kevin]: We're storing data that we don't need. We're giving access to people that don't need access. And we're doing so much online that it's augmenting our risk.

[Bill]: You bet. You're creating risk in many ways.

[Kevin]: Yeah. Well, Bill Haber, I'm so grateful that you could stop in and join us on Cyber Sip today to talk about these issues.

[Bill]: You bet. Dean will be happy to join you. And I appreciate the opportunity, Kevin.

[Kevin]: I appreciate it, too. And before we go, anything else that you want to mention that I haven't asked you about or something you want to leave our audience with that you think is critical these days?

[Bill]: Yeah, I didn't mention this as much earlier, but you did. Multi-factor authentication, MFA. Lots of people use it, but they don't use it broadly. They don't use it everywhere. They don't administratively enforce it. These are easy things to do. They don’t cost money. And everybody...here’s a public service announcement: Enable MFA broadly on everything you touch period will dramatically reduce your risk and it doesn’t cost a thing.

[Kevin]: I’m glad I asked. Thank you, Bill. Bill Haber, co-founder of TEKRiSQ. Once again, really appreciate your joining us.

[Bill]: Thanks, Kevin.

[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.