[Kevin Szczepanski]: The co-founder of TEKRiSQ is back again for a second episode. Dean, thanks so much for joining us.

[Dean Mechlowitz]: Thanks, Kevin. It's great to be here.

[Kevin]: And it's pleasure to have you back. We're going to talk about risk assessments. But before we get started, I want to ask you this question. It's really a question you presented to me. So you think that I, I'm the average organization out there—I have this enormous blind spot when it comes to cyber risk. What do you mean? Why do I have that blind spot?

[Dean]: So let's first maybe start out: what is a cyber risk. And if you're from a company perspective, if all your computers were to be shut down, would that affect your business. How it's shut down? Those are the cyber risks. But the result of your business is your computers are shut down. Or it could be if all your data was compromised and published to the dark web, would you be upset and would that affect your business? So when you sort of take it from that perspective, is how do you protect all that? And the cyber risks are the tactics that maybe companies or the criminals use to get that data. And these tactics, they go on and on. There's thousand-page books on cyber risk and how to become a certified cyber practitioner. There are over a thousand pages. So there's an enormous number of ways that can happen. It doesn't take a rocket scientist or our hacker to steal data. It's actually very simple to do. And that's why we talk about this enormous blind spot. It's not hard to do. It doesn't require a lot of technology. There's lots of tooling out there that can assist the hackers to do this. And that's why we talk about this blind spot. It's really easy to do. And there's a lot of ways that companies are compromised.

[Kevin]: So that makes perfect sense to me. We talked about the blind spot from the perspective of the threat actor. But given the enormity of these potential risks, why would any organization be callous, or whistling past the graveyard, instead of proactively addressing that? Why in 2024, does anyone have a blind spot when it comes to cyber risks?

[Dean]: Yeah. So it's a great question, but it's because people don't understand it. They think they're safe. They don't know they're set. They think they're set. They think they're doing the right things. They think the company is doing the right things. But they're not. There are some really basic things that people do incorrectly. But just going to an individual, if I ask the normal person, what do they use to keep track of passwords? They might say, well, I'm using my girlfriend's name, boyfriend's name, husband, wife, kid's name, pet's name. I cycle between those and I get really clever and put a question mark on the back side of it and call it a day. And I use it across... the standard set of passwords across all my systems. That's a terrible idea. And that's what people do day in and day out as a simple example. So they think they're okay, but they're not.

[Kevin]: All right. So organizationally, what we need to start with, and I ask you that, as a question, not as a statement, strikes me that organizationally, what we must begin with is a cyber risk assessment. Is that true? And if so, can you talk to us about what a cyber risk assessment is?

[Dean]: Yeah. So that's a great question, Kevin. So when I hear things like "I think I'm okay," "My organization must be okay because I have my IT person looking at this." "I'm using a managed service provider, so I must be okay." You know, "thinking" is not *knowing*. And there's a lot of different disciplines and a lot of expertise that's required. So because you think you're okay, it doesn't mean you're okay. And I can tell you from the, the hundreds and thousands of cyber risk assessments we've done, I've heard "I think we're okay" so many times. And there's some really obvious things that... where the clients are completely unprotected. So what we need to look at is, is how do we figure out where those issues are. What are the issues that are what are suitable for ...you know, if you can't fix everything, I mean, to fix everything, you can turn off your computers, but then you can't run a business, right? So the enemy of good is perfect. So you can't be perfect here. So it has to be really pragmatic with it. But before you do that you might have to ask yourself the questions like, well, what kind of data is my organization? Do I need to protect that data? If that data got exposed to the internet and the dark web, would that be a problem? If my computer shut down for three or four days, would that affect my business? Could I take orders? How am I protecting those systems? What kind of controls do I have in place? What kind of policies do I have in place? Yeah, if the data gets compromised, can I get fined because I'm not. I'm not meeting regulatory requirements, you know, think New York GFS or GDPR, right? There's a whole slew of regulations and HIPAA if you're compromised and you don't have the right things in place, you can be fined. And I'm sure you deal with this day in and day out and your business, Kevin. So we need to understand where the risks are in the organization from a data perspective, from a technology perspective, from a process perspective, and from a regulatory perspective.

[Kevin]: So that leads me to two questions, Dean, that I want to walk through. And then we're to talk about how you go about executing a risk assessment. You mentioned IT service providers, MSP or managed service providers. Sometimes I'll hear an organization or a client say, hey, you know, I've got an IT firm, I've got an MSP that I'm satisfied with. Do I really need to bring in another third party, another outside vendor for risk assessment? You must get that question often. What's the right answer?

[Dean]: Well, absolutely you need to. For several reasons. Number one, sometimes they're really, really good, sometimes not so good. Most of the time it's somewhere in the middle. Number two, they may not be experts on all the latest cyber issues that are happening. And number three, having an independent view of what's happening is just a good check. And I can tell you for a fact that every time we do something, we find some major issues. Well, not every time, but almost every time, we find major issues that could be easily fixed with, with a small amount of money. So having that, being sure that you're fixed and having an independent view of folks who are experts and look at company after company, and hear about claim after claim, and issue after issue, is really helpful.

[Kevin]: So one of the ideas then is that you're reviewing not only the static policies, procedures and safeguards in place, you're also reviewing the team that delivers those services. While you might not be delivering a grade on the team, you probably don't want to do that if you don't have that outside perspective. It's really hard to get a balanced and independent view on where your organization stands.

[Dean]: Exactly. And if you want to look at an example here, let's just talk about policy. So a policy without enforcement could be good. Better than not having a policy. But it doesn't necessarily mean that that's being followed. And what we found, as an example, is that you might have a policy that says, hey, you shouldn't share passwords, don't, you know...make sure they're complex, you know, change them every 90 days, you know, pick your policy. You know, when you work from home, make sure you, when you're working from home, don't use public wi-fi or things like that, but behavioral-wise, people do all those things. So unless you have the right controls in place, right, that the individuals will revert back to their bad, you know, their bad tactics and

behavior because they have no other choice. So when we look at this, not only do we look at what your policy is, but have you put the right things in place to give people an alternative to how they're going to manage it? So if you ask somebody, say, I need you to do a 20-character password, but you don't give them a way to manage their passwords, guess what they do? They make it really easy. If they write it down, they put it in an Excel spreadsheet. They maybe save it onto their... into their Google Chrome browser, you know, unsafely. Right? So they don't have an alternative. So they just they have to figure out a way to do their job and that's what they do.

[Kevin]: Right. So that leads me to the next question, which is... it sounds pretty obvious that you know, just because you have a set of policies and procedures and safeguards in place that doesn't obviate the need for risk assessment. Talk to us about why that is, because sometimes I'll get the question. Well, you know, I have a written information security plan. I have an incident response plan. Why do I need to risk assessment? I'm already past that point. What say you?

[Dean]: So let me give you an example. I'm going to change the names to protect the innocent numbers and all that. But here's an example. So a company we talked to in the same in the last month or so, they had a cyber incident, and it was it was EFP fraud. So, you know, let's say $1 million was transferred improperly. The company had a great policy in place. It said, here's our cyber awareness training. Never click on phishing links. Well, what happened was, is that the one of their vendors got compromised. So that vendor sent a phishing email saying, please log in to, your O365. Okay. That person logged in to O365. Now the hacker has access to the email, did their social engineering thing. In other words, research who does wires, or how much do they wire? Where do they wire to? Find out who was on vacation and change the name of the website was coming from by one character. Sent the email to the bank. You know, a million dollars was transferred. So they had a policy in place that says never enter your credentials when people ask for them. The policy in place to, approve wire transfers, they had all kinds of cyber awareness training in place, but that person was still fooled. So they have the policies, they have the training, but they were still compromised.

[Kevin]: So ideally, were it come to this next, ideally then your risk assessment is going to uncover the risk of funds transfer fraud. And you might conclude as part of that assessment that the most significant risk is your employees and their lack of awareness, their lack of training, lack of ability to spot these scams. And that's one thing a good risk assessment might uncover. And then you might recommend training in order to reduce that risk. So let's say we're starting from the beginning. You have a client that comes to you and says, we have these policies and procedures in place. We do our best. We have multifactor authentication. We have endpoint detection. So we think we have a good visual on what's going on in our network. Say they're legally required to do a risk assessment. Or they just recognize that it's important. And they've never done it. And they come to you... walk us through the process of a risk assessment and feel free to use as an example a particular kind of client or customer, because it does matter whether it's a regulated business, like health care or financial services, or whether it's just a small to mid-sized manufacturing firm. Take it away.

[Dean]: Sure. So let's assume for a second through some regulatory requirements like it's health care or financial, with...and they're large enough to be a regulated entity. So they have to do with risk assessment. They don't have a choice actually. In part it's like for New York, it's written into the law that you have to do one on an annual basis. So let's just assume that's the case here. So first thing we'll do is we want to understand the type of business they are. So that'll tell us what kind of regulatory requirements they may have. They may tell us that they have to do annual risk assessments, and they tell us that, cyber whereas training is mandated, you may tell us that MFA is mandated. So there's some mandates that they have to have as sort of, you know, table stakes. Next thing we want to know is, you know, kind of revenue they have. What would happen if their business was down for a day or two or a week. So we can understand what the risk might be. We don't want to... we want to understand how much protected data they have. So in techie terms, that's PII, personal identifiable information. PHI, health information, credit card information, PCI biometric information, you know, all kinds of really sensitive data. You know that if it's compromised, it's an

enormous problem for your business. We want to know where that store house is stored. Do they, do they do they store it into Google Drive? Do they sync Google Drive to their to their desktop? Do they have the right kind of antivirus in place? Right. So sometimes when they say they have endpoint, they might think that, you know, Norton 360 is appropriate, which is not. They may need to have their disks encrypted because in health care, if your computer is stolen and you can't prove that your desk is encrypted, that's considered a breach under HIPAA, for example. So we want to know, you know, where all that data is and what would happen if that data was compromised. We want to know what kind of controls they have in place. You know, are they automatically patching? What kind of antivirus, what kind of firewalls. What kind of cloud protections, what kind of MFA are they using? Are they using text-based MFA. Text-based MFA is not recommended anywhere anymore. It's been deprecated as a good factor to use because it can be fetched. More on that later if you want to learn about that. We want to know what kind of regulations do they have the plans in place to that are written information security policy required under New York law? As a matter of fact for the...

[Kevin]: DFS, the cybersecurity regulation.

[Dean]: So then we'll come up with a set a set of pragmatic recommendations of things that are prioritized to what absolutely has to be done immediately, what things they should they do pretty quickly. And what are those things they may be able to wait on. And so it's that sort of prioritized list of things they can do. And do quickly so that again, this is not their core business. The core business is what it is. This can't get it away. They still going to run it. But how do you protect that data really quickly and effectively. That's the whole goal of what we're trying to accomplish.

[Kevin]: Right. So... and every organization is different and every vendor is different, Dean. So if I'm an organization, I suppose one of the questions I'm going to ask is this sounds like a pretty extensive effort. How long is it going to take? How much of my time, not only my time as the general counsel, the CFO, the CISO, or my organization's time will it consume to complete a risk assessment?

[Dean]: That's such a great question, because usually when you think about this, you'll see risk assessments that take weeks and an enormous amount of time and a lot of cost. So the way I got into this business is I was working for, for a large telco provider, and we would sell these risk assessments that cost $400,000 and take six months. And after the six months, the main recommendation was, hey, don't share, don't store your passwords in Excel spreadsheets, right? You don't need you don't need eight, nine months to do that. It's pretty obvious about smaller organizations, midsize organizations. There's very pragmatic things they can do. We could find those things out in a half hour to an hour. So within a half hour to an hour of your time, we can find out the big hitters that will need to be fixed. Now, keep in mind, this is not a full NISC assessment or any of those really, you know, it's not like that. It's designed to be: How do I find those really pragmatic things I can put in place immediately to better protect my business starting tomorrow? And that's a half hour to an hour's worth of their time.

[Kevin]: So something efficient and cost effective and your... I wonder your reaction to this Dean? I often find myself thinking, and I think we all do this. We compare ourselves to those around us. So I say, well, how do you compare risk assessment A with risk assessment B? And one may be more detailed, one may be less expensive. But there's also another comparison which is comparing your organization today to where you were yesterday. And so I guess one of the concepts that I'm interested in, and I think you and Bill Haber over at TEQRiSK are interested in is what can we do to take this organization and put it in a stronger posture than it was yesterday? What's your reaction to that?

[Dean]: Yeah. So absolutely, that's exactly what we want to accomplish. Right. So keep in mind the enemy of good is perfect. And that would never be perfect. No matter how much you put in, you never get rid of the risk fully. But there's things you can do really quickly and effectively that are high value. Right. So think about, you know, the obvious example, multi-factor authentication, having that in place in the appropriate time. Right. That's the single most important control that a company can put in as an example. Right. So there's

things that you can do very quickly in effectively to, to fix these, these problems. You know, the things that that company X does versus company Y, they're the same things that you're going to do. It's just that some companies have a much bigger financial risk. So they may want to, you know, you know they definitely want to put them in. But the things that you do to protect, you know, your email is the same regardless of the company. Now your risk in terms of how much money you could lose could be dramatically different. But the controls, the basic controls are all the same. It's really... again, this is not rocket science. Well, not rocket science for non- cyber expert. For small to medium-sized business owner. But it's not hard to do and can be done effectively and quickly. And you can put the right controls in place and be pretty good pretty quickly.

[Kevin]: That you mentioned a few minutes ago. It's not a full blown what we're talking about now. It's not a full-blown NIST assessment. But let's be clear what you're doing is tied back to a recognized standard, either an industry standard for a client that isn't regulated or a specific regulatory standard like DFS cybersecurity regulation in New York for a business that's subject to that. Can you just talk about that? Because, yes, it's not full-on as in terms of the length of time and the significant cost, but you're still tying what you're doing back to an appropriate standard.

[Dean]: That's correct. So we're using NIST as our guideline. And what we're really looking at is anything we look at has to be actionable. Right. So if you have something in place, if it's not actionable, what does that do for you? It doesn't do much for you. So we have to do that. So we tie back to NIST, we tie it back to New York, would be to the DFS requirements so we can meet the those requirements and the things we look at are those actionable things that are high runners. And that's what we're really concentrating on. How do we action what we ask. If you ask a question, you know, and you can't do anything with that data, what's the point of asking that question?

[Kevin]: So we're coming to the end of our time. But I have two other questions I want to cover with you. First, I think it makes sense for us to transition into at least a brief discussion of cyber insurance. So you and I are...would be preaching to the choir. But let me ask it this way: How does what we've discussed—conducting the proper risk assessment and identifying gaps, implementing appropriate physical, electronic, and legal safeguards—how does that affect an organization's ability to get cyber insurance today?

[Dean]: Yes. So it actually... there are certain things in the cyber applications that are absolutely critical, if you don't have, you might get cyber insurance, but it'll be limited. So based on the threat you... they may have sub-limits. So typical sub-limits are. Yes claims and ransomware. So there's a lot of other things in the policies. So what we want to do number one is we want to make sure all the right things are in place to ensure that that cyber policy, they get the best terms they can for, you know, where they're at. That's number one. Number two, keep in mind cyber insurance is a risk transfer strategy. So the reason we have it in place is to reduce risk off the company. But also keep in mind that even when you have it, it's still, you know, having an incident. It's not something you want to do even if you have cyber insurance. So we want to make sure that we're covering the risk transfer piece, making sure that sails through, make sure the underwriters understand, you know, the right kind of controls are in place. But also, more importantly, trying to avoid the claim in the first place. So it's absolutely critical to, as part of your risk transfer strategy to have it, for a variety of reasons and having the right kind of controls in place before you even submit really helps with that process.

[Kevin]: So I'm going to have a guest on in the coming months, I think, maybe even weeks, who has written a couple of books, one on this issue. He is very strongly against the cyber insurance product, and he comes at it from a macro level. And, I'm going to be digging more to his position as I get closer to interviewing him. But essentially, his point is cyber insurance is not long for this world. And the reason is that underwriters have nowhere near the amount of data they need to properly underwrite cyber risks, particularly catastrophic risks. And so anyone thinks who thinks that cyber insurance is a risk management tool they should be thinking about is crazy. Now, I think the listeners and viewers of the Cyber Sip podcast will know that I don't agree with that, but it's an interesting concept. So I want to close with this, I'm putting

you on the spot. What question or point would you make to this mystery guest who will be on later this year in response to his thesis that cyber insurance is not what it's cracked up to be, and it's not long for this economic world.

[Dean]: Well, there's a few things of this. So first thing I'll do is I'll just take a real pragmatic minor, the theme here. Pragmatic. How do you be pragmatic? Say a company, let's say you have a say you're, you know, $30 million in sales, you got 80 people, and you're hit with a cyber incident and you have no insurance. What do you do? Who do you go to? Who's your incident response team? Who's on the panel for your lawyers? Who's going to take care of, all those notifications you have to do? How many states are you doing business in? Right. Oh, you're in California. You're in Colorado. You are in New York. You have some business in the European Union. What are your notification requirements? So trying to navigate that without having a wingman, like a cyber policy and, and that panel of experts, I don't know, that could be a problem. If you know, how much money would that cost you? The average cost of a record breach, I think, depending on where you look, 150 bucks a record. Right. So you don't need a lot of records to be breached where it could be really hugely expensive. So, yeah, there are issues with systematic risk. And those things... just look what happen with CrowdStrike. But cyber insurance provides a really needed function to help those businesses that, if they were to be compromised, they wouldn't even know where to start. Yeah. Where do you even start? And the cost associated with that could be enormous and put them under. There's statistics that show that small businesses are hit a lot of them go under after a cyber incident. So thinking about sort of the big picture, what's going to go a long term that doesn't really help the small guy or the medium-sized business today.

[Kevin]: I think those are great points. And I think the last point is the best one, even if you believe that long term, systemically, cyber insurance is not going to last. That doesn't answer the question of the business owner who suffers a data breach tomorrow and who doesn't have cyber insurance to transfer the risks of investigation, notification, legal analysis, defense in a data breach class action. So there's big picture, as you say. And there's the small picture that thousands and thousands of small to medium-sized businesses really care about most today.

[Dean]: Absolutely.

[Kevin]: Yeah. Well we're going to leave it there. But Dean, thank you so much for coming in and being a guest once again on Cyber Sip. Yes, I do know the name of my own podcast. I misspoke, but no, seriously, thank you for coming in. Really appreciate it. I hope that everyone who listens to this episode has a renewed interest in cyber risk assessments, because it really is the starting point for an overall cyber hygiene that's going to protect your business from the risks that it faces really, every second of every minute of every hour and every day.

[Dean]: Absolutely. Thanks, Kevin.

[Kevin]: Dean, thank you so much. 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.