Barclay Damon Live **Presents** ***Cyber Sip™***
Season 3, Episode 3: “Why You Absolutely Must Do a Risk Assessment in 2024,” With Bill Haber

Host: **Kevin Szczepanski,** Barclay Damon

[Kevin Szczepanski]: Hey, everyone. Welcome back to Cyber Sip. I am very pleased and honored to have back on the podcast Bill Haber. Bill is the co-founder of TEKRiSQ. Welcome back, Bill.

[Bill Haber]: Thanks, Kevin. Great to see you.

[Kevin]: It’s great to see you, too. We are going to talk today, Bill, about why you absolutely must, must do a risk assessment in 2024. I think a lot of our friends out there running businesses, especially small ones, get the cart before the horse. They want to talk about the security controls like multifactor authentication, smart passwords, encryption before they’ve actually taken a hard look at their computer systems to see what they have and what they need to protect. So let’s put the horse before the cart, and let me ask you first, what is a risk assessment?

[Bill]: Sure. Fair question. And that’s probably a great place to start. A risk assessment is, is simply the process of identifying hazards that could negatively impact an organization’s ability to do business. They should be exercises that are designed to be extremely helpful in the identification of very specific business risks. And when done properly, they should prompt leaders to adopt new measures or processes or even controls that reduce the impact of those risks. And we focus on cyber-risk assessments. So they look more specifically at how a business uses technology and things like who has access, how do they handle data and exchange it, how do they protect themselves from cyber risks, and how do they plan to operate going forward? And there’s a lot of ways to do them internally, performed by external parties, but they should always be kind of conducted by qualified individuals who have strong knowledge, good judgment. And something we talk a lot about, which is pragmatism, something that’s sensible and realistic. You don’t do a three-day, $15,000 risk assessment for a small company with a simple tech stack and just a handful of people. So it should match the company. It should be pragmatic, come from qualified individuals, and be extremely helpful to the organization.

[Kevin]: There’s a lot of stuff there I want to circle back to, Bill, but one point that I think is worth mentioning is that as an organization, you can conduct a risk assessment on your entire computer system or you can focus on a particular system like your mailbox, your Outlook system, for example. So you can calibrate your risk assessment to your budget, but you should absolutely do one. I shouldn’t say that first, Bill, let me ask you this: Is there any reason you can think of that an organization, even a small business, should not be conducting some form of risk assessment?

[Bill]: No. I think risk assessments are extraordinarily helpful and too few businesses do them. I will tell you something that we’ve seen this year that’s probably important to share, and that is what a risk assessment is not. And...

[Kevin]: Great...

[Bill]: One thing it's not is a simple external scan. Some companies that do these, they basically display the electronically observable data about how your domain is configured or errors in your settings. And they're beginning to call those things cyber risk assessments. That's not exactly a cyber risk assessment, and that should only really be used as a term for assessments in very mature technologies environments where all the machine-controlled devices are connected, and data is at folks' disposal. But for most companies, a scan is not an assessment. But having a good professional perform that is absolutely critical and it's becoming more important every day.

[Kevin]: Thank you for that, Bill. I think that's a great point. And I think I will add to that by saying that simply having a series of security controls in place like MFA, smart passwords, endpoint encryption, you name it, there are... we become dangerous knowing these various security controls. But simply having those in place is not a risk assessment, either. So if we're thinking about... we're trying to tell our audience how a risk assessment works. Can you at a high level, walk us through how this happens and let me start off by asking, is this something that can be done in-house or is it something that should be done using a trusted outside vendor with experience in these? I think I'm probably giving away the answer, but is it something that can be done in-house or is it a more elaborate process than that?

[Bill]: Well, it depends on why you're performing it and what type of organization you are. I was going to talk a little bit about why they're necessary and why most businesses need one more specifically.

[Kevin]: Let's do it. Yeah.

Bill: Cyber risk assessments are increasingly necessary just to do business. You're seeing that board level and business executives are now expected to have visibility of all business risks. And they haven't always looked at the technology risks. But if a breach were to take place (and I think businesses need to start looking at when they will happen rather than if) and so when they happen, that can impact liabilities, reputation, even things like valuations of companies. And so they don't always have the people, particularly in smaller companies they invest in. They don't always have the talent, the time or even the objectivity to perform these reliably. And businesses have always been assessed on things like their credit profile with things like Dun & Bradstreet reports or assessed on their reputation, their propensity to pay their bills, things like that. Now they're being asked by insurers and other trusted advisers, like lawyers and accountants, even by companies that they're doing business with—their trading partners and regulators from all ends of the globe, from other countries, from different states, from the SEC and Commerce Department, even municipalities like the New York Department of Financial Services—to conduct these periodically; have them done... file that they've completed them and show that they're following recommendations. So there's kind of this new, converging compliance thing happening and fines are starting to reach the millions and they're being issued and publicized. So that's a whole new area of business risk. And when you ask the question about in-house versus outside, I would say this, Kevin, that if you're an organization with a really mature technology stack and a lot of internal resources, perhaps you have a chief information security officer and an internal, mature cybersecurity team, those people are well-trained and often regularly conduct cyber risk assessments internally. They participate also in external audits from SOC2 and beyond. So, you know, they implement means to benchmark and measure improvements on an ongoing basis. But we find most of our work is with small and medium-sized businesses (think of companies with 200 employees or fewer) and they find that they often don't have those CISOs, they don't have a cybersecurity team, and that third parties give them impartial, pragmatic, and affordable ways to do this, hopefully tailored to their business. We do different risk assessments for like health care organizations then the standard ones we do for different types of businesses. So yeah, we focus on making them more affordable, pragmatic for the small and medium-sized businesses.

[Kevin]: And just thinking... building on that, Bill, is the point I touched on earlier. I want to get your reaction to it. Ideally, we'd like to see an organization conduct a risk assessment of their entire system. But if you're a small organization, you don't necessarily have to do that. If there are budget constraints, then can you focus on certain aspects of your system, like email or maybe the storage of PHI, if you're a health care service provider. Have you seen that? And would you recommend that an organization conduct a risk assessment even if it's only a partial one?

[Bill]: So I would never advise a company not to conduct one in any part of their business. I do think it's important to find vendors who can give you a holistic cyber risk assessment that is simple and focused on the core issues that they need to look at. I mean, we have a version of our cyber risk assessment that takes a half an hour to assess the organization and is extremely affordable. And you should look for vendors who offer that. Not everybody who performs these is focused on making them accessible to everybody. Some of them, you know, we oftentimes joke that they'll produce a mountain of paperwork that nobody's going to read, and it becomes unactionable. So the key is to make... to create a powerful, useful cyber risk assessment, you've got to look at what matches the organization. And we try to do that.

[Kevin]: So let's dive a little bit deeper into what a risk assessment looks like for our audience. And let me first ask you about that 30-minute assessment that you mentioned a minute or two ago. And then maybe we can expand on that and talk about what the more elaborate risk assessment looks like. So first, that what does the 30-minute risk assessment look like and how can that help?

[Bill]: Sure. Well, what we like to do is we like to meet face-to-face over Zoom or other technologies to have a discussion with clients and make it a relaxed process where they don't necessarily feel like it's a test or quiz, because that's not what it's supposed to be. But we like to walk them through a few topics and make sure they understand what's being asked of them. Sometimes self-assessments or online assessments can produce poor responses or un-useful data because people don't understand what's being asked of them, or they might have a misunderstanding or an overstatement of fact. And that's all bad. So we like to speak face-to-face with people, and when we conduct a half an hour assessment, we want to understand, we want to identify both in their industry and in their organization where risk exists, how well it's being mitigated. If there's any risk that we see that isn't being mitigated and, make actionable, pragmatic recommendations. What do we mean by that? That's typically understanding where issues exist and then following up with a set of recommendations that are appropriate to their organization and maybe simple things like you mentioned earlier, enforcing MFA administratively, that's something that anybody can do fairly easily. They don't necessarily need to have any technology assistance to do that. And we often give folks instructions on how to do that. Potentially we'll request that they look at more significant security controls. This can be things like endpoint detection and response which, to obtain insurance and protect the organization, are becoming more and more useful and popular. Encryption tools, using MFA or VPN broadly across the organization. And oftentimes we'll look at an organization in terms of what are their policies and procedures; are they even in place? Do they have documented policies and do they tick the right boxes that people expect to see in an organization? So we might recommend that they go and find vendors or, you know, some of those things we do... a lot of those things we partner with. But we will recommend that they put some of those policies and procedures in place. That's also can be critical to obtaining the right insurance coverage.

[Kevin]: Right. As we're talking about risk assessments, not only for the purpose of obtaining and maintaining your insurance, but also to protect your data, protect your dollars. We're seeing a lot of funds transfer fraud, and also to limit liability. So it's not a question of whether you'll be attacked. It's a question of when, and if you're... you have an organization that suffers a data breach, you have to disclose that breach to affected individuals. You have to report it to the attorney general or some in some cases more than one attorney general. There are often investigations and data breach class actions. And by conducting a prudent risk assessment ahead of time and putting those controls in place that you're talking about, you can limit liability because you can explain in response to these investigations and court proceedings that essentially that you acted reasonably and you complied with the appropriate security controls, right?

[Bill]: Yeah, that's absolutely right. And sometimes it's just a matter of, in those processes and procedures, noting that in the event of a breach or some incident, that there are compliance issues to follow up with.

There are notification rules. I think you've seen headlines recently, Kevin, where folks have, you know, have otherwise mature technology teams and cybersecurity staff who sometimes blow those things off and focus on mitigating the risk recovery and years later, they end up getting fined sometimes millions of dollars by every state because they failed to follow all the procedures that are expected. And so it's important to have plans documented that folks can follow when there's a breach, everyone's hair is on fire and everyone's just focused on what's the most urgent thing. But you really have to do a thorough job because there's a whole level of risk on the back end, if don't.

[Kevin]: So before we talk about the more elaborate risk assessment, it just occurred to me that we may not all be on the same page. I think you and I are, but everyone watching or listening right now might be thinking, okay, we're talking about a risk assessment. What's the risk? Give me an example of a risk that we have to assess. So let's talk about that now. And I guess I'll start off and then I'll let you run with it. One that we see is the risk of business email compromise. And when we're thinking about these risks, Bill, maybe tell our audience we're not just thinking of risks academically. We're evaluating those risks for gravity as well. So there may be risks that you have in your organization, but there may be... there are risks of different levels. A ransomware attack, for example, might pose an existential risk, whereas some risk of upgrade in hardware or software has less of a risk. So I hope that makes sense. I'll turn it over to you if someone's listening and thinking, okay, I've got to do a risk assessment, but how do I decide what my risks are? How do you address that?

[Bill]: Well, you know, we'll look at things like... so you used business email compromise as an example. That's increasingly something that's impacting small and medium-sized businesses. So when we perform risk assessments, we'll ask people, you know, how do you use email, what do you have in place? Are you doing anything to block or mitigate the risk of receiving phishing attempts or business email compromise where deception is involved? Where your employees who—oftentimes it's the employees who are fooled or tricked into clicking something or exposing something. So what do you put in place? Do you have anything in place? And oftentimes, they'll say, oh, well, we have some spam tools or email filtering, which can be very useful, certainly is better than nothing. We like to look for, you know, are you training your employees? And are you educating them on things like business email compromise and phishing and how people do it? Are you blocking new domains? DNS blocking, or DNS filtering is a common tool that's used to prevent that. And we'll look at anything that they may be doing to minimize that risk. And if they aren't doing anything or doing very little about that and they have a large employee base or a lot of folks interacting on the phone or operating using email, which many companies do, and that's something that needs to be called out. So I hope that's a good example.

[Kevin]: No, it is. It's helpful. So, Bill, for organizations who... we talked about the 30-minute risk assessment, sort of like a SWOT [note from the editor: SWOT = strengths, weaknesses, opportunities, and threats] assessment that you do at TEKRiSQ, could you contrast that for a moment with a more detailed risk assessment that other businesses with perhaps more time, more resources might consider? What does the more detailed risk assessment look like? How long does it take? What resources are necessary both in the organization and outside, to complete that assessment?

[Bill]: Sure. So there is no shortage of large enterprise risk assessments that often find their way into medium-sized companies that can be performed over months; can take a segmented view of each part of the organization, talk with multiple appointed individuals, and go through what we regard as a lengthy set of questions and answers that most individuals don't have that data at their disposal. So they can take months and costs tens of thousands of dollars. And at the end, sometimes they produce a copy of what looks like "War and Peace" written in Sanskrit that doesn't always find its way into the actionable space where the management team in the boardroom make real decisions based on it. Because it's essentially just getting through a large homework assignment, but large, mature organizations with a CISOs sometimes have those performed. They often do it themselves. You know, one of the reasons why we've brought our risk assessment process forward is we have some experience working with organizations who perform those, and it's often really clear what the most pragmatic cyber risks are that need to be, that… where action needs to be taken and specific areas that can happen very quickly in the… even in these lengthy risk assessment processes, you can see what organizations need to do. But yeah, there are certainly companies that can do those over months, weeks, days. And we've kind of brought the cyber risk assessments that we do down to, you know, from that half-hour risk assessment to a 90-minute enterprise assessment we do, and about an hour for health care organizations where we kind of just look at the most pragmatic things and make recommendations that are actionable. So, you know, nobody's that distracted and folks can get that out of the way and plan on doing that on a regular basis.

[Kevin]: So when you complete that 30- to 90-minute process, you get some results. And what happens next? How do you take what you've learned, what you and the organization have learned and translate that into actionable steps?

[Bill]: Sure. Well, we produce a couple of reports that are really useful to a number of folks, but particularly the companies that we're assessing. We'll produce an executive summary. And we think it's really important to strip a lot of the technology and cybersecurity jargon out of that and focus on business outcomes and plain business language. People can relate to that. And it just calls out, you know, these are the… we actually highlight them with, you know, with red text and say, you know, these are the things that deserve attention and here's why they impact your company. And we recommend that you do the following things, either from a solution standpoint, from a configuration standpoint, like configuring MFA, or put some policies and procedures in place. And then we sometimes are able to propose some of those solutions or will refer folks in some cases that can help them to take those actions. And we'll also create cyber risk reviews that are a little bit more comprehensive, a little bit more "techie," and even accompany those with things like insurance applications, and supplements like ransomware supplements and other things. Because often the folks that we're working with are seeking to insure their organization. And once they have the assessments done and maybe take a few of these actions and we'll revise that that reporting and then help them use that in their insurance submissions, which can be really useful. I think underwriters like seeing that a third party has taken a look at this, has made some recommendations, and the companies have responded to it. So we kind of bundle that all into a process of tech risk. But yeah, other folks have different processes. I think making it actionable and helping folks to correct these issues when they identify them is really important… as long as you're not asking them to do something that is beyond the scope of what they're really going to do. Cybersecurity, especially foundational cybersecurity, shouldn't be a headache and it shouldn't break the bank. It should be done incrementally and throughout the business cycle to make improvements and show progress and become more sophisticated over time.

[Kevin]: Very interesting. No, that makes perfect sense. And it leads me to this question, Bill. When you're in the recommendation phase of a risk assessment, how do you explain or justify the recommendations that you have? Let's say, for example, their security controls, and we talked about some of them earlier and that they endpoint detection and response. There are other examples. On one hand, we know there are heavily regulated entities in the financial industry, in the health care industry, that may be subject to federal laws in health care, for example, HIPAA, HITRUST, HITECH, but let's say we're dealing with a small- to medium-sized manufacturing company, not subject to financial regulations, not subject to health care regulations. How do you go about determining which controls, for example, to recommend? And how do you explain to the CEO of that company that these are things you need to do, even though there isn't a law somewhere that expressly requires you to do it?

[Bill]: Yeah, great question. So, Kevin, it can be very subjective and depending upon what people do in the course of their day and what they have access to. If it's a manufacturing organization and they're doing some type of highly skilled manual manufacturing, that's one set of concerns. If they use industrial control systems and software that is used broadly across an organization and they don't have the proper cybersecurity controls in place, we know that vulnerabilities are sometimes exploited in those systems. So if we discover that, we'll make a whole different set of recommendations about what they need to do to protect folks from accessing those systems. I just saw the other day that there's an attempt to breach a number of wastewater management systems widely deployed in the United States that an Iranian organization is behind because they're seeking to make Israeli manufacturers look bad in the eyes of US businesses. So that's a particular instance where a nation-state hack comes down to medium-sized businesses and wastewater facilities all across the country are having to worry about this, and make sure that they put the right controls in so that they can protect themselves.

[Kevin]: Yeah.

[Bill]: So it's discovering what are they using, who has access to it, and how are they protecting that access. Sometimes there's not very complicated systems in use and there's some basics that we'll recommend. Other times, you know, there can be significant risks. We'll call them out and explain what we think they should do to get themselves out of the crosshairs.

[Kevin]: Right. And I think from a legal standpoint, I'll just add that even if you're not a regulated entity, a financial services company or a health care company, if you have data, if you have data of individuals, you're obligated to protect that data. And if you suffer a data breach and a threat actor is able to access or steal that data, you're going to be subject to the breach notification laws of every state in which you have an individual client or consumer. So whether you are required to follow some established regulatory scheme or not, this is a negligence standard and you have an obligation to act reasonably. And I think increasingly we're going to see in 2024, if an organization hasn't done a risk assessment, they suffered a breach and an investigation or a lawsuit reveals that the security controls were inadequate, you're going to be liable for fines and penalties. You're going to be liable for judgments and settlements. And if you have cyber insurance, you may find it very difficult to keep it. So there are a lot of really good, strong reasons to start with a risk assessment and to go from there in in setting up the security controls that you need to protect the data that is so critical to your business.

[Bill]: Yeah, absolutely. And you know, along those lines, Kevin, some folks don't realize that regulators in Europe have policies where if you are providing services or some type of access to a user who may live in the United States but is a European Union citizen, you now have a compliance responsibility with GDPR. If you are selling products and services and you happen to sell them in New York or California or states who have some stringent new regulation, you're on the hook. So you've got to understand who you're doing business with and what that obligates you to do. And risk assessments help call that out.

[Kevin]: Right. And it's a team effort, right? Bill, you've got your inside IT or information security teams. You have perhaps outside forensic teams and you also have your either in-house or outside counsel. So you have information security obligations, you have forensic investigations, and you have legal obligations. It all fits together. So I think that's a great point to end on. Bill, I want to thank you for coming in to talk about why you must do a risk assessment in 2024. I think this is so important. And I think what you do is so important, and I look forward to having you come back on, look forward to seeing you and Dean later this year.

[Bill]: Awesome. Thanks, Kevin. Happy to be on the show. And yeah, I agree with you. Anything we can do to help. People can find us at TEKRiSQ.com, T-E-K-R-I-S-Q dot com.

[Kevin]: Appreciate it. All right. Well thank you, Bill Haber, really appreciate your joining us and thanks to all of you for joining us for this latest 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.

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.

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.*

Thanks for listening.