Barclay Damon Live Presents *Cyber Sip*™ Episode 44: "Your Cybersecurity Roadmap: Targeting Gaps and Assessing Risks," With Brian Haugli

Speakers: **Kevin Szczepanski**, Barclay Damon, and **Brian Haugli**, SideChannel

[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]: Everyone's super excited to have on today's episode. Brian Haugli, CEO of SideChannel. He is the founder of RealCISO, the creator and host of The CISO Life Podcast, which you can find on YouTube where I have found it, and I assume, Brian, wherever fine podcasts are sold. He is also a cyber evangelist and educator. He was a professor of cybersecurity at Boston College a while back—probably before he got so busy that he can no longer do everything. But we're grateful that he's here today. Brian, welcome to *Cyber Sip*.

[Brian]: Thanks, Kevin It's a pleasure to be here. I always love talking about this stuff, obviously.

[Kevin]: I know you do. And just before we get started, you've got it. If you haven't checked it out, if you check out Brian's LinkedIn page, he has a.. his first... this is your first "press conference" as a "head cyber coach." Brian, I put it out on my page as well. If you haven't seen it, guys, you want to check this out. And Brian, I thought you did very well. You managed to answer questions or not answer questions while sounding like you were answering questions. So is just like an NFL head coach.

[Brian]: Thanks. Yeah, we had a little bit of fun with a new character. And it's always interesting when you're the CISO at an organization and I draw on that from my days in the DOD and in a Fortune 500. When you're being asked questions maybe by board members or other leaders in a company about what's going on, and I just always thought it seemed like it would be better suited to be in a press conference style, or ...it is almost the same thing that a head coach is doing after a game. Win or loss. Just getting bombarded with questions and people are just ask... like drilling you for info and you're sitting there trying to represent, you know a win is a win. And yet some people are like, well, you didn't win by much. Why not? You're like, but I still won and you sort of bring people through it or explain why you got the loss and it wasn't as bad. So it was just some fun we're having. We're looking forward to doing more.

[Kevin]: Before we talk about risk assessments too Brian, tell us about your new book, not so new anymore—I think it's been out for about a year, but I was so excited to see it when it came out. Tell us about your book. What's the title and what is it about?

[Brian]: Yeah, so it's on risk management. It's published by Wiley, I'm a contributing author with Cynthia Brumfield. And the book is entirely around the practical application of meeting the next cybersecurity framework or the NIST's CSF version 1.1. And actually we know that version 2.0 is actually out right now for comment, and they've introduced some governance controls and things that were lacking. But really, you know, the purpose of the book was not for someone with my background to read it and go, oh, okay, I like... it's not geared for somebody with my technical depth. It's actually geared for people who aren't or who do have the technical that, but it's really built around, hey, listen, here's what the NIST cybersecurity framework, CSF, is looking for. And in each side of each of those controls, how do you meet them? What is a

practical application? What's a tactical and technical implementation that you can put forward? What type of people, what type of process? What type of technology should you be thinking about to meet each of the 108 controls? And so we wrote this book to kind of give people that guidance because everyone wants to follow a framework or a standard, and yet people have a hard time actually meeting it because they don't necessarily understand, well, how do I prove that I meet this control or that control? So the intent of the book was really to guide people and give them some background and ideas about how to think about meeting each of the controls within the NIST CSF.

[Kevin]: Yeah, I think we're going to talk more about that a little bit when we talk about risk assessments. But before we get to that, and I'm not going to say anything, for those of you that are listening, you should watch this episode if you can. For those of you that are watching, I'm not going to tell you what's coming. But if you're familiar at all with Brian, you know what's coming. Before we talk about what a risk assessment is and why it's important, and what it comprises, I want to dispel a myth. And I think in some ways, those of us who are or consider ourselves to be cyber evangelists, we have unwittingly perpetrated this myth. And the myth is, you know, there are half a dozen or dozen or so security controls, multi-factor authentication, smart passwords, endpoint detection and response. And there are we could go on. And if all you do as an organization is check those boxes and implement those controls, you've got nothing to worry about. True or false?

[Brian]: That's false.

[Kevin]: Why?

[Brian]: So, and here's where it gets fun, right? When you get into the applications, right. Of tools, we're really centering around technologies and processes, not really people, not governance, not anything else. So you could have a number of capabilities, EDR, good passwords, maybe email security. And I'm never going to say these are bad things to do, but yes, I implemented them. Okay, great. Governance and having a cyber program is what takes all of these components from being just "we implemented that tech. We're good." And going from "we implemented it on day zero. Is it as effective on day 300 or day 3,000?" Are there any degradations of this capability throughout this timeline? Are there new threats that maybe have made this capability less effective? Do we need to expand this capability to new users, to new systems? Has the accreditation boundary for our environment grown? And governance—and having and running a program—and this is the core to what a chief information security officer is supposed to do, besides shepherding the narrative to leadership about the program, the goal of the CISO is to govern that. The program that's in place, the technologies we selected to implement, are as good on day 300 as the day we implemented. And all these other aspects of what's changed inside of environment, the program has kept pace with it. Because you've identified a risk on one day and said these are the risks that we want to reduce or hopefully remove. Well, great, If the environment changes, that risk might get worse or much more of a priority or much more of a risk. Are your controls as effective? Are they keeping pace with that risk as it changes? So when you take the compliance approach and say, yep, we just did this, we did this, we did these things, we're good, you discount any changes in your environment and you discount any threats external to your environment, to you. And governance is all about addressing those two things and managing that as a program. So that's why, you know, compliance is great, but it's the foundation of the program, it's what you need, but it's not keeping pace with what your organization is doing, what the risks are that mean something for you as an organization that you need to be aware of and stay on top of.

[Kevin]: Yeah. So the place to start is not at the end with the security controls, but the beginning. And that's what we're going to talk about today. So we don't hear it said very often. But I think the most critical place to start is with a risk assessment. So I know you can... walk us through what it is, Brian, and then maybe if you could distinguish between an overall, what I'll call an "overall" risk assessment and perhaps a more targeted risk assessment. Right, because you can do a risk assessment for your entire system or you can focus on a particular application or your employees or something more discrete.

[Brian]: Right. So, I mean, risk assessments are the nature is going to be the same, whether it's micro or macro. [Drawing with erasable marker on clear board throughout episode.] So let's take an organization here and you have a set of servers, applications, databases, people, right? And they're all happy people.

[Kevin]: Of course.

[Brian]: This is what you're responsible for. You've also got probably access and dependent on third party capabilities, third party vendors.

[Kevin]: Like the cloud...if you have data.

[Brian]: Yeah, you have vendors that are sitting working for you, you've got infrastructure that sits in a cloud as well. This is your accreditation, this is what you're responsible for. And everybody who's just listening and again, I'm drawing on a board here, so it's to show this. So you are missing out on some aspect of it, but I'll talk you through it. This is what you're responsible for. Okay? When you do a risk assessment, it's in kind of a couple of parts. And again, whether it's that single system or this organization as a whole, my job—and I'm always taking this from the approach of I am your chief information security officer, what am I doing? How am I thinking about this? I am looking at what the posture is of this organization and I am looking at what the outside risks are to the organization. And you have to address them separately, but you can't do them independent of each other. You can't do one and not the other and expect you're going to have a good outcome. So when I look at the internal organization, the reliance, what we'll just call it, kind of like our accreditation boundary. In the government, it's commonly called to an accreditation boundary. This is what's in this. Anything outside of this is out of scope I'm not worried about I'm not assessing. What I want to do is, I want to do a controlled-based assessment and do a gap analysis on those controls. Now, what is that? I'm going to have to pick a standard. Okay? I can't just look at this and go, okay, what feels right? Because if I do, I'm actually making a new standard. And let me tell you, the security industry does not need another standard. Okay. So for all intents and purposes, let's say you're following the NIST cybersecurity framework. CSF. Okay, this you could follow ISO 27001. You could use a compliance framework like the HIPPA Security Rule or the FTC Safeguards Act or New York State, DFS Part 500. These all have a list of controls and what is a control? A statement that you have to meet. Okay. But let's just pick, you know my favorite because it has 108 controls that we can look at. Now what am I doing? I am looking at this organization through the NIST lens and figuring out, out of 108 controls inside this accreditation boundary, which ones can I say I meet? That is a gap analysis against a control framework. I am looking at the internal part of the organization. Okay. It's not actually a risk assessment, it's a control assessment. So I figure out I'm meeting, let's just say, you know, 90 of the controls. Okay, so I know what I'm doing. Great. I have 18 controls that are deficient. That means I have 18 controls that are in my gap. Now, I look at those and I say, is this, is this good for us? Basically, you could say, look, 90 is good. These 90 that we're addressing are the 90 we want to meet. The 90 represents your current state. Okay. If you say, listen, we actually want to meet, there's ten of these 18 controls we want to actually address because we feel like that will be the posture we want. That represents your target state. So you have your current state and your target state. Okay? The path in between? That is your roadmap. So I've identified ten controls I want in my roadmap to address. So that becomes... now projects that becomes resourcing, right. That's people, process, and technology to address those ten controls on your roadmap from your current state to your target state. That's your internal organization, that's your area of accreditation. Okay. The external component, the risks are outside of your organization. What are the things that are going to impact me? What do I need to worry about that are outside of my control? Do I need to worry about advanced persistent threats? Do I need to worry about nation states? Am I a target? Am I in a supply chain for, you know, the Chinese and Russians that have their eyes and concerns on me. Maybe, maybe not. Do I? Am I worried about ransomware as a threat? Am I worried about business email compromise as a threat? These things can happen to me because I have an email server that somebody can get into, because I have infrastructure, someone can ransomware, but are they risks that could happen to me that I now need to prioritize and look at and say, okay, that is something. Ransomware is a top risk I am worried about. All

right, maybe data loss is another risk because I have intellectual property and I have, I feel like a weak HR capability to look into the backgrounds of individuals. I feel like I have insider threat and I could have data loss. Do I...You know, these are these are your external risks, right? So you factor in these external risks and you bounce them against basically what your controls are. And now that further informs prioritization of the controls. Now you can go say, hey, listen, in fact, I need to do 15 of the 18 controls I'm not meeting, because I've looked at the risks externally to my organization. And this, ransomware, is my number one risk. That's a problem for me. And I see that a number of these controls I wasn't previously looking at would address ransomware as a risk to me. Now I need to include that into my roadmap, into my gap analysis. Right now, you can see why some organizations... will do one or the other and they'll miss the other aspect.

[Kevin]: Right.

[Brian]: And they won't get a... because the end goal of anything is to have a roadmap towards a target state. So you can't have a fully built roadmap unless you actually know your external risks and your internal controls. So this all informs kind of what your path is. So me as a CISO, Fortune 500 or, you know, smaller organization as a virtual CISO, I'm looking at an organization through this lens that, okay, this is what you now need to do, right? Thankfully, you as a business have decided you want to do the right thing. You don't feel like your security posture is where it needs to be. You want to make it better. But how do you know where you're going to spend your vital resources to make it better? How do you know that priority one, the priority one control, the things that that is going to close the most amount of risk to you, is your number one? Or are you unfortunately spending your time and money on priorities numbers five, six and seven. So this type of an approach allows you to prioritize your resources appropriately, take a methodical approach to having a risk assessment done. And all of this, right, all of this becomes an auditable artifact for you to prove to anybody. Shareholders. Yes. Executive leadership.

[Kevin]: Regulators, plaintiffs in class action lawsuits...

[Brian]: To say, we thought about this, we looked at our current state, we figured out what we looked like. We figured out what our risks were as a priority. We built a plan and we started resourcing and marching towards that plan. We made decisions based on actionable data. And I can't tell you how many organizations don't do that. Many, many organizations that SideChannel starts with, they'll say, oh, we did something like this, and you go through and you're like, you did half of one of these and not the other. You did one, not the other. You didn't do either. And you just kind of said, this feels right, finger in the air, and you're kind of doing something because maybe that's what sales sold you, or maybe that's what somebody's friend said this was good and this helped them, and... it doesn't work that way. So I like this methodology. I didn't invent this methodology. This actually stems right out of a lot of what NIST and standard risk management frameworks do. But it is amazing that, you know, as much focus and attention cybersecurity gets, we don't actually implement the things that cybersecurity industry has put out as the kind of the best way to do that. So again, not mine, but this is just how I apply it. And I can tell you it's worked with everyone we go with because it's a solid methodology.

[Kevin]: So couple of questions, Brian. One is maybe more hypothetical than real. When you were talking about the initial analysis and then the risk assessment, I was thinking to myself, well, what if hypothetically, my organization has already complied with all 108 of the NIST security controls. Do I even need to do the external risk analysis? Because the result of that is simply going to... I don't have any gap to fill. Or is the reality, and the more likely scenario that your... the organizations you are working with have not complied with all 108. They've complied with a fraction of those. And the risk analysis helps you prioritize, let's say they've complied with 50. The risk analysis helps you prioritize which of the next 58 controls you need to comply with to address those external risks. How does that work?

[Brian]: Yeah, the prioritization is always going to be helpful if you're deficient in meeting your target state. So that's going to apply any time. I'll say to your first part of your question, even if you met—from a compliance

standpoint, you said, yes, I do all 108. Okay, what's the efficacy of each of them? How mature are each of those controls? Because the risks... like you might have kind of a baseline capability inside of all of those controls. You might be meeting... you just meeting them or you just got something that you can kind of put forward and say, yeah, we have something in that inside that control. For me to say we've got that covered. But maybe the risks external to your organization have moved so much or just changed just enough to make what you've done for that control insufficient. Okay. For instance, last year the Verizon Data Breach Report, which is a phenomenal canon of work put out every year, I think showed that business email compromise surpassed ransomware as a external threat and risk. So what does that mean? That means that everyone had been focusing on ransomware as a risk to address for so long and probably had BEC or some... a little lower down. Well, now the bad guys figured out there's a much better there's a whole different discussion on how that works, but BEC is a much better ROI for the bad guys. So that's more which means that as a, as an organization, I need to be focusing a lot more on my email security because that is taking uptick. Well, to answer your question right there, that's a perfect example of how the industry shifted. Both the bad guys and the good guys shifted in how they address a risk that now became number one. So yeah, it's... there's a level of maturity within each of the controls that you constantly have. And again, that's back to governance, right? Me, me as a CISO running a cyber program, I am constantly thinking about am I doing ...is everything I'm doing inside of my target state controls or my current state controls? Is it enough? Should I be looking at other technology, should I be bettering my processes? I mean, I'll tell you this you get into an incident, right and good incident response obviously gets through the incident, but it does a postmortem, it does an after-action review.

[Kevin]: No, absolutely.

[Brian]: You will always go and sit there at the table when you're looking around and everything's settled. Hey, what can we have done better if you come out of an incident response and there's like, now there's nothing we could have done better.

[Kevin]: "We're good."

[Brian]: I mean, God love you, you're amazing. But I've never come out of an IR where there wasn't some type of, hey, we could have done this better or that better. That's maturity. That's looking at what you're doing today and saying, next time we can do this. So we're better. Right? And reducing the risk, reducing the impact, you know, you're never going to really necessarily reduce the threat. Right? The threats are always going to be out there, but you can reduce the impact or even the possibility of it impacting you.

[Kevin]: We've only got a few minutes, but I want to ask you two questions before we go, Brian. So much more we could discuss. One is a quick question, and that is if an organization is interested in starting from the beginning where they should, conducting this internal analysis and risk assessment, is this something that the average small to midsize company can accomplish internally with their existing IT staff, their existing information security professionals, or is this something that's better left to a third party vendor who can come in and independently review the status of your network and controls?

[Brian]: So I have to be transparent, right? Because I run a consulting firm, SideChannel, that focuses on mid-market companies and small businesses to do this. We are a third party to those. The other piece, and I'll kind of pick on what you said a little bit, Kevin, unfortunately, but most small businesses, even mid-market, don't have internal security practice.

[Kevin]: That's true.

[Brian]: That's honestly been a lot of why I started this company was to address that because it was a... it's a very underserved market. It's very hard for mid-market small businesses to be able to attract, let

alone retain, these individuals with this skill set. So could they do it? Yes. If they had the... if they had the resources, do they know? Because they don't have the resources? That's a lot of it. What we built with one of our pieces of software with Real CISO. So was trying to give the CISO with a small team the ability to actually do this themself. So, you know, you don't need software from us necessarily to do that. You can do this in an Excel spreadsheet. You know, it's just not scalable. You're going to hate it after a while. And this is coming from somebody, you know, 20-plus years in the industry. You started out doing all of this stuff in Excel. It gets old real quick. It doesn't scale, it doesn't allow you. So there are solutions out there. Right? And again, transparency, like we built one, but there are solutions out there that will help you make this happen. So having an IT team, right? Is good. Having security people who can focus specifically on this is better. But yeah I mean it's been...I see a combination when you're in the larger organizations, when you're really truly in the $5 billion plus enterprise revenue space you've got the team you've got a CISO right. Because again you think about it like, you know my starting salary as a full time CISOs East Coast, half a million, West Coast $800... or yeah $800,000 on the West Coast... just to have that leadership role. It's not cost effective for that mid-market. So it's really cost effective, it works out for the larger folks and then they can start having teams and they can start doing this internally. But really that I've been seeing about $5 billion and less in revenue space, it becomes very difficult to bring on that type of talent and effectively do this. So where you can outsource because it traditionally will be much more cost effective, but it's not necessarily... Don't think you're abdicating your responsibility for cybersecurity by using a third party. It's still your responsibility as an organization. You should still really kind of be very much in tune with that third party that they are aware of and aligning to what your business objectives are. Goals right, and protection kind of goals. Is it brand, is it identity? Is it revenue? Is it key customers? Right. What are you trying to protect as a business? A third party can only tell you the types of things to think about. A third party, I can't tell you which one is the one that... it's your business. You need to tell me: what's important to you. Your brand revenue. These three clients, whatever it is, and then you work around that. So yeah, I definitely get into some of these conversations with businesses and they're like, oh good, you're just going to... you own all of that. So yes, I will mechanically run all of this for you. But at the end of the day, you still own this responsibility as making sure cyber is in place.

[Kevin]: Well, Brian, I think that's... thank you so much. I think that's a great place to leave it. We're out of time for this episode, but I'd love it if you could come back. We've got so many other things I wanted to ask you about. I want to talk about Evil Proxy and the assault on MFA and cyber due diligence and M&A transactions. But we will leave that for another day. Will you come back and talk to us about those sometime?

[Brian]: Definitely. We'd love to.

[Kevin]: Well, Brian Haugli, thank you so much for giving us your time here today. We appreciate it. Look forward to having you back.

[Brian]: 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.

Thanks for listening.