Barclay Damon Live Presents *Cyber Sip*™
Episode 45: "Building Trust One Deal at a Time: Due Diligence in M&A Transactions," 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]: We're back with Brian Haugli, who is making his second appearance on Cyber Sip. Welcome back, Brian.

[Brian Haugli]: Thanks, Kevin. Pleasure to be back here.

[Kevin]: CEO of SideChannel, founder of RealCISO, and creator and host of the CISO Life Podcast, which you can find on YouTube and wherever fine podcasts are sold. Brian is back with us today to talk about cyber due diligence in M&A transactions, something that has become increasingly important. But it's been around for a while. Brian, tell us a little bit about how you get involved and what you're looking for. And let's be even more specific. You're on the side of the acquiring organization.

[Brian]: Right.

[Kevin]: So what are you doing? And walk us through it.

[Brian]: So what I like to do is anytime we're doing an assessment, whether as the organization part of the organization or as a consultant to the organization to help them through this process is ideally—this is the idea and this doesn't always work out—but ideally, the organization itself is already following some type of cybersecurity framework or standard. You then want to be able to assess any asset to that standard. Why? Because at integrate, if you're going to integrate that asset into your organization, merge networks, merge capabilities, it becomes a lot easier to then kind of overlay map in, bring that in because you're assessing them against what you're doing. You know, where their gaps are. So, you know, if your capabilities they have in your organization can now just overcome any of the gaps inside of that acquired asset or not. But you don't necessarily have to. Maybe the sub organization or the org that you're looking to M&A is following something themself and you just want—for ease of use—you want to assess them against that standard that they're already aligned to. But let's just take a kind of an overarching kind of risk assessment/gap analysis type of a process to the asset. Now, we do work with organizations that are acquiring assets to bring in. We do work with private equity companies that are looking to invest in assets, and they're going to keep them as wholly owned subsidiaries like, PEs do. What I've learned kind of out of the gate with deal teams is and this is going to be unfortunate for some people to hear, but the cyber posture of an organization rarely, if ever, sways the deal maker from wanting to do the deal. So my approach has always been to do the assessment on the organization, figure out what the gaps are that they are, that they have. Right, so they have these things. They don't have this. And instead of using that information to dissuade a deal or put... cast negative light on the asset, instead figure out what the cost is to address meeting that gap. Because what'll happen now is, you know, the deal team is going to want to do it. Okay? Whether it's the PE guys and girls or the team at the organization for a merger, they can factor that into the deal price and that becomes huge leverage now, right, for the organization because if this is an area that needs to be addressed. Okay. Say they don't have MFA in place or they don't have email

security and that's going to cost money. Well, now you can say listen to the asset, us buying you is going to make you where you should be, because you don't necessarily meet a standard or our standard of security or even an industry best standard, we're going to need to invest money to be able to make you whole, to bring you up to our level. So this has been a very, very well-received approach. And quite honestly, I don't see a lot of other groups out there who are supporting organizations or PE in the M&A process around cyber due diligence actually taking this approach. They take that, Well, here are the gaps. I'm trying to give the deal guy reasons not to do the deal. Stop. Just please stop. Take more of a practical approach and help the deal team make the deal, right, and bring the asset in. Now, that's kind of just the overarching really, you're doing a risk assessment of the asset, right?

[Kevin]: Right.

[Brian]: You pick. Yup. You pick this CSF, right. And you kind of run through the controls. What is the asset? What does that company what are they doing? What are they not doing? What falls out becomes the gaps. You can then put costs, resources, timelines against how to meet those gaps. Post-acquisition, maybe it sways them. Maybe it's the organization. They want to do this as a merger and bring them in. Maybe this gives them enough information to say, listen, you're gonna be a wholly owned, separate network, separate entity until you become whole, and then we'll be able to bring you in. Right. But there's a lot of things that can go wrong if you don't even do due diligence around cyber. You could be inheriting an asset that is already compromised. You could be inheriting an asset that has such poor capabilities, it's going to be a gargantuan task to be able to take... to be able to really move the needle post-acquisition. And if you don't factor in these costs beforehand, well, now you're sitting on the other side of the deal. You didn't resource for it, you didn't build that cost in, but you still have to address the gaps. So you're either going to accept the risk of the asset as it is, which is not a great idea because there's some deficiencies that could cause you risk, or you're going to have to spend money that you otherwise weren't planning on to make that organization whole.

[Kevin]: So in that last scenario, Brian...where the risk is more severe? What are you seeing out there? Are you seeing—I know you mentioned earlier that as a general matter, the investor, the acquiring company is not walking away from the deal. But in that narrow situation where the asset is really not up to par, there are, and a significant investment will be required. What's the breakdown? Are there acquiring businesses that will walk away from a deal? Are they... or are they looking at simply adjusting the price to account for the work that will need to be done after closing?

[Brian]: It's the adjustment. I mean, five years of doing this as a consulting firm and supporting companies in this, I have yet to see an organization walk away from a deal because of a poor cyber posture of a potential asset. It's just not happening. Right. So it really is getting them to understand what is the cost to make this thing whole, right. Bring this thing to a standard. And again, you're the overarching entity. You can bring this in and say, yeah, we're just going to accept all the gaps that are there. Maybe because we're just going to move entirely off of some of their infrastructure. And those deficiencies only exist in that legacy infrastructure. So we're going to get rid of it. That's fine. That's one way to do it. They could accept the risk as is and integrate it. I don't ever recommend that. But again, that's a business decision, right? And my job is to inform the business on what the merits are of what they're doing, where the risks truly are, what could happen if the risks manifest not only for the asset, but the organization as a whole. But ultimately, that is a business decision there, and hopefully my job is to sway and influence them to make something that is much less of a risk to this entire process and to the end state organization.

[Kevin]: So in our first episode, we talked about the importance of and the execution of risk assessments. And I think you alluded to this earlier, but it almost sounds like what you're doing is a form of risk assessment when you are looking at this, you're looking at the asset's security controls.

[Brian]: It is. I mean, it's I don't believe in the due diligence realm, it should be anything different or separate. You should be assessing this organization against some type of standard. NIST, ISO. Maybe the asset you're

acquiring is in health care. Well, does it meet the cybersecurity requirements under HIPAA? I mean, that's... out of the gate that you should figure that out. So it's this is a standardization, right. And I don't understand why. I think there are some of my peers out there who just kind of, "this feels right, let's do this. This is our magic process." The industry as a whole spent a lot of time and got a lot of the smartest people in rooms together to come up with some of these standards and agree on them. We should use them. And doing an assessment of a cybersecurity posture of a potential acquired asset is no different than assessing the organization you're in itself and what its cybersecurity posture is.

[Kevin]: Right. Right. If you're so... it's almost silly not to do not to assess the asset because if you're assessing yourself and you're planning to bring this asset into your own organization, you want to make sure that what you're bringing in fits your security controls, fits your model.

[Brian]: Yeah, the thing you don't want to have happen is you've spent a lot of time and resources as an organization to better your security posture and then acquire an asset that degrades your security posture. Right. Why step backwards after you've already spent time and resources to move the needle forward?

[Kevin]: That's the risk. I was going to ask you that. But that's the risk of not doing this. The risk is that you are going to be subtly and ultimately degrading your own security posture.

[Brian]: Yes. And the worst case, though, is you're actually acquiring an asset that is already compromised. And we've seen that where we've done technical deep dives, threat hunting inside of acquired assets only to find out, hey, your email server or your file server has malware or control system on it that is controlled by somebody that's not you. And you're literally now walking that into your organization if you do some type of integration.

[Kevin]: Right. So I want to I want to ask you about reps and warranties insurance. So this is funny, I remember being a young lawyer. I don't want to say how long ago this was and someone asked me about reps and warranties insurance and frankly, not many carriers were offering it. It wasn't a thing. Today it's a thing. So I won't ask you that. That's too easy. Right? I want to ask you about moral hazard, though. So reps and warranties insurance will function to safeguard your representation. So if you are the asset and you're representing that you have X controls in place or that you have reasonable safeguards in place to comply with all applicable laws, including privacy laws and Gramm-Leach-Bliley and FTC safeguards rule, whatever the whatever the law may be. I just wondered your take on that in some ways, do you think that either party to the transaction ever makes the mistake of assuming they don't need to upgrade the safeguards? They don't need to do the risk assessment because if anything bad happens, the reps and warranties insurance will be there is a backstop, so close enough horseshoes and hand grenades... close enough, enough to worry about it. What's your take on that?

[Brian]: You know, I don't think I've ever been asked that question.

[Kevin]: Good! That's good.

[Brian]: I would equate that almost to, you know, I'm an organization. I built the basics of cybersecurity and I have a cyber insurance policy. And I'm looking at my cyber insurance policy to just take care of any deficiencies that I overlooked or I felt was reasonable enough. It comes down to when I file a claim. Right. Does that scenario play out in in the claim itself? Right. So I think in this... in the same way when you're when you're looking at your reps and warranties, you kind of have to look at, hey, let's come up with a hypothetical here that happens to this asset or to the organization. Right? It manifests. Would the reps and warranties cover it? I don't think I would look at it just like, oh, it will cover it. And I feel good enough, like work with your broker. I mean, we do this with... we do this with our clients right now where they'll say, oh, we have cyber insurance. Like, okay, great, let's get your broker on the phone. Let's walk through a scenario, a cyber scenario.

And I want my... I want your broker to tell us if that's covered. Plain and simple. And we get a lot of folks who are surprised. Some are unfortunately surprised that the broker doesn't know actually how to do that. And if that ever runs your way, go get a new broker. But if you do get a broker that runs you through that scenario, they're like, oh, actually based on the exemptions and the policy, this scenario wouldn't be covered. And you kind of have to look at, well, how real is that scenario to manifest and why? Is it because we have risks that we didn't think about? Is it because we have control deficiencies we didn't address? We need to do something or we need to get that not exempted or we need to somehow up our cyber coverage to be able to do that? So I think you need to be able to walk through that same type of process with the reps and warranties, like, hey, if... the... what we addressed inside of and what we found is gaps actually manifested as a problem, would the reps and warranties cover it at the end of the day?

[Kevin]: Yeah, no, I completely agree with you. That is the right way to look at it. I think that some small to midsize companies get confused and think it's one or the other, or they think that if I have the insurance in place, I don't have to worry about the other. I don't have to worry about assessing the risk and having... mapping my controls to a recognized standard like NIST. And the reality is that both of those things are increasingly inextricably linked. You are not going to get the insurance that is going to safeguard your risk unless you've been able to demonstrate that you have those controls in place, that you have assessed your risk, and properly applied controls to manage that risk. So I think that's absolutely right. If anyone ever did think that insurance is a panacea for managing cyber risk, I think we know today and if not, we should, that is not the case. And in fact, as you point out, you can lose your insurance if you haven't implemented the security controls that you've represented to your carrier that you have in place during that application and underwriting process.

[Brian]: Yeah, exactly. Spot on.

[Kevin]: Well, Brian, thank you so much for stopping in talking about this due diligence issue. It is critically important and I really appreciate your taking the time.

[Brian]: No. Thanks again for having me on. Pleasure to come back any time.

[Kevin]: No, no, it's...the pleasure is all here. And thank you. And thanks to all of you for joining us on this 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.

Thanks for listening.