Barclay Damon Live Presents *Cyber Sip™*
Season 4, Episode 8: "Understanding Tech E&O Coverage: A Guide for Businesses," With Damion Walker

Host: **Kevin Szczepanski**, Barclay Damon, and
Damion Walker, Gallagher

[Kevin Szczepanski]: Hey everyone, Damion Walker is managing director of the technology practice for Gallagher, the third largest insurance broker in the country. He has 20 years of financial and insurance experience. Before Gallagher, EVP with Willis Towers Watson. Before that, SVP at Hub International. And before entering the broking industry, Damion was an underwriter for AIG, controller for an international glass manufacturer, and financial analyst for global consumer goods manufacturers. So, we're so happy to have you, Damion Walker, on Cyber Sip.

[Damion Walker]: Hey, thanks for having me. Pleasure to be here, Kevin.

[Kevin]: Your extensive experience, I think, before you entered the broking industry, how informative was that for you when you started with Hub, Willis Towers, and now with Gallagher?

[Damion]: So I think before I joined—actually, like many of my colleagues, I got into the insurance industry completely on accident. I was going to grad school to be an analyst. I was employed by a glass company. I was doing controllers and whatnot, and I was recruited by AIG to come in. And I think having that background in credit, in finance, allows me to kind of see insurance differently. Like we've discussed earlier, I don't kind of see it as a lawyer, I see it as a financial tool. I've kind of grown into the lawyer side of it. But I think that allows me to kind of see insurance differently, how it helps our clients use it as balance sheet protection, eliminate the volatility in their business. And then of course, making sure that contracts and their business function properly. So the insurance is supporting their business, not necessarily just buying insurance so that they have that protection or they're buying it because they have to—but really leveraging the insurance to help support the business and the growth of their operations.

[Kevin]: Yeah, it poses legal issues and encroaches that area, but as a risk management tool, really is critical to business operations. So I'm glad we're going to talk about it today. So before we get started, let's not assume that everyone understands it. What is tech E&O coverage, Damion? And since I think some people sometimes confuse it with cyber insurance coverage, maybe explain the key differences between those two different insurance products.

[Damion]: Yeah, absolutely. So I think it's funny because even in my own practice, we call tech E&O, you know, cyber, right? It's just easier to refer to a cyber. We talk to the markets about it. We refer to it as cyber. And that's because what technology E&O, you know, insurance is, is it's cyber insurance for a tech company. So tech companies have a very unique exposure in that their professional liability—so their delivery of technology products and services can lead to a cyber issue. So when you issue a tech E&O policy, the foundation of a tech E&O policy is professional liability. So you are protecting your client from an error or omission in providing technology services or products. Now, how the product has evolved over the years is you've now stacked cyber coverage on top of that. So now you have the full suite of an error and omission that might lead to a technology issue that causes a cyber breach or a downtime in your network or downtime in a customer

network. It protects...it's an umbrella that protects a technology firm from any type of professional error and or data breach, malware issues, network outage—as one umbrella so that you don't have two different insurers pointing a finger at one another saying, no, no, no, the professional liability caused the issue, not the cyber breach. So I need you to cover this part and I'm going to cover that part. So about. 2008, 2009, it became very commonplace for technology companies to marry those two coverages under one policy covering professional liability and cyber liability. And now, you know, back then there was four or five insuring agreements. Now I think the last one we placed has like 16. So it covers a broad breadth of the exposure from the professional liability side, it covers media liability. It covers all the security and privacy issues that you get under a cyber policy. So it's a very broad-breadth policy covering a lot of different apparels for a technology company, not just cyber.

[Kevin]: So just to clarify then, Damion, would or could that cyber or that tech E&O policy include an insuring agreement that provides first-party cyber coverage for data breach, ransomware attacks and so on?

[Damion]: Yeah, good questions. Yeah, so. It's funny when you work with a lot of government agencies or we have clients that work with government agencies, they want that policy to be separate because they want that first-party coverage for your customer. And they want third-party coverage as well in case my client causes a data breach or some type of network outage on the next site. So the policy covers all of that. So there is... back in the day, there was this disconnect. They thought that the cyber on a tech E&O policy was "cyber light", right? It wasn't true cyber coverage. That didn't contain all the bells and whistles that a true cyber policy covers. Now it does. There is full, it is full coverage in, I would say even more broad coverage, broader coverage than what you would find on a traditional cyber policy. Because technology companies have broader issues, right? They are providing software, they are providing services, they are providing network components that help your company run its cyber infrastructure. So even if you're not a [garbled] company, your company is a hundred percent reliant on your email. Like most of us. You even if you're not in the tech industry, if your email goes down, you're like, I'm might as well go home for today. Right. So my clients, a lot of my tech clients, they basically provide those services that make your network run. And if they bring down your network, you know, they're liable for not only their issues, their professional services and/or the cyber liability for bringing down your network. They also have the cost of bringing down their network if that occurred as well. So it's a very broad brush, first party, third party. You can even get some non-IT service outage provider coverage now. So there's a lot of different coverage that can be added to a tech E&O policy.

[Kevin]: Mm-hmm. Right, so Damion, do clients who come to you, do most of them know they need tech E&O coverage with a cyber component or are there times when you have to make the case to an organization that, you know, look, this is a product that you need to fill a gap in your insurance program?

[Damion]: So I would say, so it's funny, if you look back, even five years ago, we had a lot of clients that were buying no professional liability or some kind of light professional liability, and they were buying a cyber policy as a tech organization. I would say in the last three to five years, that knowledge base has grown either through the brokerage community or the clients themselves have become more sophisticated. The large space is [garbled] spot tech E&O for a decade. But in the middle market space, I would say in the last three to five years, most clients are aware that they buy tech, you know, they don't necessarily know what that means. They don't know what the insuring agreements and all that are, but they know that their cyber coverage covers their professional liability as well. So I would say most folks are now up to speed on tech E&O. Now the only place that does differ is outside of the United States. So if you have a foreign parent that's domiciled in India, Singapore, China, even some, some of the Baltic States, you'll find that in those countries where the insurance market is not as robust, that you'll still find clients that are buying professional liability and cyber, particularly in India is where we run into it a lot. So as that market is developing, they're starting to use London more more and more, but you'll still find parent policies outside of the US that are covering US risk that are separate professional liability and cyber. They're traditionally with the same carrier, it's usually an AIG or Tata, something like that.

[Kevin]: Right.

[Damion]: Outside of the US, you'll still find pockets where clients are buying both professional liability and cyber. But within the US, most clients are now buying tech E&O.

[Kevin]: So talking about that… it's good to hear that the market is increasingly sophisticated. That's helpful. And I know what you mean about…the difference or the supplement of domestic-side insurance with insurance, particularly in India. So I guess in some ways this leads well into the next question. And you and I have talked about this before and it may be a delicate subject, but I'm asking you anyway. If I'm an organization, I'm a CFO, can I purchase this coverage on my own? Do I need to go through a broker? And if I do need to go through a broker—and I assume you're going to tell me that's a wise choice—how do I know I've found the right broker? There are a lot out there, many to choose from, but not all created equally, especially in this space. So how do you talk clients about choosing the right ambassador to go out into the market for them?

[Damion]: Yeah, so that's a complicated question actually, and it depends on the size of the firm really. So there are a couple of unique markets out there that are positioned to help tech startups, if you will. And you can go online, the client can go online without a broker, fill out an application and get really good, viable coverage. There's a couple of markets that are really, really good at issuing startups. Now there is an issue with that coverage in that it does lack some of the coverages that we can negotiate as a broker. It traditionally is a little more expensive. It's easy to get to, right? You can just go online, buy it. You can be contractually compliant in an afternoon. It generally costs a little bit more and it lacks some of the coverage disciplines that we see as a broker. So as you know, as you grow, maybe you buy that the first couple of years you're running, it's not a big expense. It's four or five thousand dollars. Maybe you're buying a very small limit. But as your organization grows and your customers are now saying, hey, I want contractual liability up to like $5 million, I want you to start buying larger coverage, you kind of outgrow that self-buying mechanism. And then you've got to go out and find a broker. And my recommendation would be to find a broker that has specialty brokers that do just cyber, are just tech E&O. And again, I just saw I mixed those two together. But the reason being is, that the market is fluid, not only in pricing, but in terms and conditions. There's always new coverages being added, lately it's been wrongful collection are non-service provider power outage–type coverages. So there's always something unique that's being added to the market that a broker will see. Now, if you go to a non-specialty broker, let's say you go to a broker that runs a small shop in San Francisco that doesn't necessarily have that specialty resource, they might go to a wholesaler, which is a third party that would broker that placement for them. But wholesalers traditionally are kind of placing very quick coverages. They know what enhancements are available to them, but they may not press for you. So we find that wholesale placements are usually generally good in terms of pricing. They're okay in terms of their terms and conditions. But if you go to a broker that… knows your business, markets your business and the understanding they have with you as a client, and then has direct relationships with the cyber market, both on the claim side as well as the placement side, you'll have a better cyber experience. And then, God willing, if you do have a claim, if they have claim services, that's even a better benefit for you because there's nothing more difficult to handle than a cyber claim.

[Kevin]: You're talking about the importance of getting to know the potential policyholder's business. And I think that dovetails with the question I had for you. Let's assume that the client has found you and you've got to take the step to, you're eventually going to go out in the marketplace and try to obtain quotes. What do you do vis-a-vis the client? And similarly, I suppose, what are the underwriters of the cyber and tech E&O carriers looking for it. How do you marry those things together? Make sure that your client is best positioned to get a cost effective and complete quote from more than one carrier.

[Damion]: Yeah, no, absolutely. So I would say this is probably one of the most important things that we do, right? So we bring on a new client, they're buying a tech E&O policy. So we look at that policy, we see if it's priced right, if the terms and conditions are at market. But the next thing, very next thing we do is we log into the client's website, and we take a look at all of the services they provide and the underwriter will do the same. Part of the next …part of our data collection processes is we ask for a complete cyber application. It is a

daunting task for many insurance. It takes multiple disciplines across the company to do it. Your IT staff needs to be involved. Your financial staff needs to be involved. Legal needs to be involved. It's quite an application. And then we also do a ransomware supplemental because we want to know what your controls look like from a ransomware standpoint. So that gives us a good foundation and the basics of what your company looks like. Here at Gallagher, we also do a network scan. So we want to see what your cybersecurity controls look like from an outside perspective.

[Kevin]: Can I just interrupt real quick, Damion, I hope I'm not ruining your train of thought, but you mentioned an external scan. That's more and more prevalent. Can you walk us through what that is and how is it that Gallagher has the ability to do that?

[Damion]: No, absolutely not, great question. So it used to be back in the day, back in the day you'd fill out like a three-page application.

[Kevin]: Like three years ago, yeah, you can get cyber insurance like...

[Damion]: Back in the day like two years ago. Piece of cake, right? And the underwriting was very limited. There wasn't a whole lot. And then the market took a bath. The cyber market was very hard, '21 to '23, because the underwriters were taking a lot of losses. So they put in a lot of backward network checking and tools to help them assess your security protocols, just like you would a building, right? When an insurer takes over the property insurance on a building, do you have a front door? Does it have a lock? Does it have sprinklers? The insurance companies from the cyber side need to do the same thing. So they run with an external network scan and they're looking for things like, do you manage open ports well? Do you have good encryption security? Do you have all the door locks that we expect to see on a traditional firm? Is your patching cadence good? Are you putting new patches on your software? There's lots of things that insurance companies can see from the outside and some have built their own proprietary network scans to check out insureds and then others outsource it. There's companies like BitSight, Securia Scorecard, and a few others that the insurers outsource, which is something that we do. And it's really important for our insureds to know that well in advance, because if you go to an insurance company and you have open ports or you have bad patching cadence, we want to say that we've addressed that security issue and let the markets know that this outside-facing network scan... that we've identified this issue, we're resolving it or have resolved it. And therefore we're a better security risk than the firm down the street. And you should give us better insurance at a better price. So I think it's really important that we do that. It's become more commonplace in the last couple of years, but I think educating the insureds so that they understand how the insurance company sees them as a risk, just like they do on auto or property or any other line of insurance, is incredibly important. So bringing that network scan is really important. And like I said, there's several resources that companies can use to do it on their own or through their broker.

[Kevin]: So you talked about some of this, and I want to drill down on it now. And I hope I can use the phrase red light, green light. So good and bad. What are some of the green lights that underwriters will look to to say, this is a risk that we can support. And on the other side, and you can take them in any way you like, what are some of the red lights where carriers will look and say, either we've got to sub-limit this, raise the premium or worst case, we can't insure you at all.

[Damion]: Yeah. So, like I said, a few years ago, you had four-page applications, no big deal. Now ...cyber insurance, I think the reason why losses have gotten so much better over the last three years is that insurance companies demanded that insureds had certain security controls. And one of the very basics that's come up is in an identity access management tool, MFA. We're all familiar with it, right? When you log in to a new website, you have to put in your username and password, then it sends you a text, right? And it says, here's your security code. So this is no longer a, "we like to see you have this." This is a "you must have this," right? You must have this tool. Um, things like, you know, really good backup procedures are incredibly important. You want to have off, you know, off-premises backups. have to be run regularly and not only do you have to

have them, they want to know that you've checked them. Do they actually work? Right? So if you do have a ransomware event, can you get to your backup tapes and get your business back up and running? Cause that's, you know, a large part of the loss in terms of a network breach. I talked about patching cadence and vulnerability management. Then I would say one of the big ones for me is, do you run phishing training for your employees? Do you have a site security annual training? Because most errors are still caused by people clicking on that wrong link or having a website that you can access that you shouldn't be able to get to from your protected corporate network. These are things that insurance companies now are demanding that our clients have and without kind of having those basic set of tools in your toolbox, then you can't even get coverage. Now we're starting to see kind of that next progression and they want to see access tools, something like, you know, email filtering. Is, are you running an email filtering tool to block phishing and that kind of thing? Are you running a PAM solution, which is a privileged access management solution? It's that only people that are supposed to have access to different data or different networks actually have access to those and are you logging it and checking it? So we're seeing this progression of the insurance companies making sure that...tech firms and normal folks buying cyber insurance have the right tools to protect the organization. Again, I always lead it back to property insurance, making sure you have the sprinklers and the lock on the front door and all that good stuff. I think considered continue to see this adaption. If we talk a lot with our clients: where's the next investment I need to make in my security architecture so that I'm compliant, so I can still buy insurance? It's not no longer, well, I have a higher deductible or why I have higher pricing.

[Kevin]: Right.

[Damion]: It's more about can I even get insurance because I don't have the right security protocols. So super important to continue that investment. And we talked a lot about investment versus insurance trade-offs. It's discussion every year with most of our CIOs and CTOs.

[Kevin]: So Damion, what if, and feel free to use an example, but let's say I come to you and I think I'm a large business... if I'm coming to you, but this applies equally to SMB, small and medium sized businesses. What if I come to you and said, look, we just had a claim, we've had a ransomware attack. Good news is we were able to remediate; we're back up and operating. Bad news is, you know, we don't have insurance or maybe we had insurance, and it wasn't renewed. If you're in a situation like that, some clients will come to me and say, you know, I don't know what to do to get back on the nice list, to get off the naughty list and get insured. Or in other scenarios, the client is afraid to report a claim because they're concerned that if they report it to the insurance company, they're going to get dropped. What do you say, what do you do with a client who comes to you with that problem? Is there a way to get on the nice list again and be insured if you've suffered a loss or you've lost coverage in the past.

[Damion]: Yeah, so again, so I think if you look at the market, if this happened back 2020 to 2023, you'd be on the bad list. You would be non-communicado to the cyber market for a couple of years at least. The good news is that because of the better controls, because of the better security environments in most of our corporate infrastructures, the market has experienced a lot less losses in the last couple of years. So even if you have a significant loss as an SMB, as a small firm, the question would be is: what security measures have you taken? Have you hired new staff? Have you put in better software? Have you better your patching cadence? Whatever it is, whatever caused the breach? How did they get in? What have you done? Have you started doing more phishing training with your employees? Whatever caused that breach, what remediation steps have you taken? What's in place? And then, you know, what have you done that's going to stop that from happening today? And there's 43 cyber insurers now, give or take. The market is extremely beneficial to insurance buyers right now. So even if you've had a large breach, number one, always report it. You don't know the extent of that breach when it occurs. You don't know what the fines and repercussions of that breach are going to be. So report it, right? So if you don't exceed your deductible, great. The insurance company's not going to hold it against you. But in today's market, even if you do exceed that deductible, if you want to stay with your current insurer, yeah, you're going to get hit with a 25, 50% premium increase and maybe doubling your deductible for a year or two, but the penalties are no longer there. They're not as punitive as they were a

few years ago where you just couldn't buy insurance because I had a breach. No, can't buy insurance. Those days are not ...in the current market that's not really happening. We've even had some insurers that have had a major breach rectified all the issues, hired a new CTO done several things. And at renewal, we actually were able to hold everything constant. No increase in premium, no increase on retention. It's about working with the insurer and telling them what you've done on that security, the backend. And your broker should help you frame that. Your legal counsel and your broker should frame that to the insurance companies saying, here's what happened. Here's the wonderful things that we've done. So this will not happen again. And you know, we'd like you to, we'd like to still be a client. And if you do all those things right, the market is very receptive to continue doing insure you and not having some massive penalty, you know, because you've had a reach. To me, I personally think if you got hit pretty hard, the chances of you getting hit pretty hard again in the next couple of years are pretty low. So you're actually a pretty good risk from that perspective, right? And that's how we frame it. I think most markets see that. It's very rare that you'd have a $5 million breach two years in a row. You know what mean? Even for an SMB, it would be really weird to have that happen.

[Kevin]: Yeah, I think the lesson is if it does happen, when the inevitable breach does happen, do the right thing, report it to your insurance company, remediate it correctly, focus on that post-breach upgrade period where you're implementing those, not only those electronic, but physical, administrative, and legal safeguards, you're going to shore yourself up, brick yourself up for the next, not only the next event, because threat actors are attacking us all the time, but also for the renewal period. So let me sidetrack you a little bit. We're getting close to our time, but I want to ask you that "what keeps you up at night" question. So what's your biggest challenge these days, Damion? I suppose that most of the clients that come to you don't need to be hard sold on the need for techie E&O coverage, but what is the biggest challenge you think you and the industry is facing right now? It is, if it's not a soft market, it's an ever-expanding market. So people should be getting this coverage. It's helpful and important. What are some of the challenges that you face?

[Damion]: So I would say the biggest challenge we face and the thing that keeps me awake at night is some of our larger customers and some of our smaller customers, they bring on new services, new technology products during the year and don't tell us. So we have clients that... let's say they're a software provider primarily and then four months after renewal, they decide they're going to start doing some payment processing. So all of sudden they start doing some payment processing, which requires a whole other set of safety tools to protect networks and your clients' networks. And they didn't tell us about it. And then three months into that, no, all of sudden they have a breach, right? And they've had an issue or they brought a client's network down, one of their customer's networks down and we get a notice. And I was like, I didn't know you did that. And we didn't tell the underwriter you did that. Now, in all things in reality, there is coverage there, right? There is coverage because it is a related technology product or service, but the underwriter didn't underwrite it. And it just makes that claim more difficult. And I will tell you, all of our, I especially love our smaller clients that are just out of that startup mode that are bolting on services. They're becoming successful. And maybe they do a financial software that is now doing payment processing or they're adding payroll processing. And they're doing something unique that diversifies their risk exposure, but we didn't tell that to the market. And I was not aware of it. Those are the things that kind of keep me awake at night because I hate to have that claim come in and not have my insured know that they are covered. And also my carrier partners are important too, as well. I want them to know what they're insuring. So when a claim does come in, we're all clear. This is what my client does. This is what happened on the breach, and it's insured. There's nothing worse than not being able to tell your client definitively on a Sunday morning when they've had a that, yeah, you're covered, this is what we need to do. And generally it's the lawyer that calls me and says, hey, my clients notified us, you know, this is confidential, blah, blah, blah are we covered? And they're like, well, this is what happened. What are they doing? They're doing business in India? We had no idea. We thought they were only domestic. So. Those are the interesting calls that come in. you know, I think the important thing is for a broker, we try to stay in touch with our clients at quarterly basis at a minimum on, the, not just talking to the CFO or the treasurer. I want to talk to the CTO. What is going on? What are you doing? What are your challenges? Are you switching? Are you a PAM solution? Like, what are you doing? What can I tell the carrier as an update if necessary? Right. We don't need to, you know, overwhelm the carrier with

updates, but that's what, you know, if you ask me what keeps me awake at night, that's really what it this proliferation of our client services that start to fall outside the scope of what we think...

[Kevin]: Right.

[Damion]: ...We underwrote, what we think we're covering. You know, it's sometimes it's professional services. All of sudden, you know, they're only offering software, but now they're installing software on client premises, right? It's, those interesting, unique things that clients do that, you know, I hate, I, it hurts me inside to tell clients they don't have coverage when just because we didn't know that's something they were doing. This is new.

[Kevin]: What should they do in that situation, Damion, if they find themselves expanding into a new line that they didn't discuss with you or as part of the underwriting process? Should they follow up with you and discuss it and then you decide whether some additional information needs to go to the carrier? How does that work?

[Damion]: Yeah, no, absolutely. I mean, that's the point. We try to schedule ongoing calls, especially with the CTO, right? That's the important side from the technical side. But staying in touch with the client, and quite often, if it's a bolt on, if it's something kind of minuscule that changes their proliferation. But we have clients that all of a start offering insurance services. Or they start offering, it's not quite tech. they're offering something just a little bit outside the professional liability realm. We talk about it and we say, yeah, this is covered. This is why we're going to tell the carrier, but you're doing this. This is, this is your, the, you know, where you're indemnified under your policy. But sometimes we're like, no, this would require a separate policy. It's probably going to cost you a couple thousand dollars because this risk falls outside of the policy's definition of technology, products, and services. So when that happens, like I have a financial client that started doing some collection activities—collection activities are not insured by most tech E&O policies from a professional liability perspective that requires a separate professional liability policy. staying in touch for us is critical, especially when have businesses that are doubling in size every year. Those are the most fun to work on. The clients are super dynamic. But it's always good for a business owner, a legal counsel. You guys would probably know before us, they're signing a new agreement. This is not a traditional service they offer. How about your broker? Tell them that you're doing this. Make sure that you're covered. That's it.

[Kevin]: Mm-hmm.

[Damion]: Being upfront about exposure is better than hoping you have coverage of the back end.

[Kevin]: Yeah, agreed. All right, we're almost out of time and probably not enough time to talk about this. But before we go, I wanted to ask you about contractual indemnification and additional insured status. These are hot topics. We encounter them all the time, whether we have the vendor or the organization with the vendor, when something happens, inevitably, the first thing we hear of it is a demand for indemnification. And very oftentimes there's a discussion about whether the vendor's coverage provides additional insured status for the organization. Talk to us a little bit about that. What are you seeing? What considerations need to be thought through before the insurance is issued?

[Damion]: So tech E&O coverage is probably the most important coverage a technology client buys. It's probably the most expensive, right? From a limit perspective. So the last thing I want to do is give a third party right to access my policy. Now, most policies will have built in provision for additional insured rights under the cyber portion, right? So they can access it for cyber breaches and file a claim on your policy if you go bankrupt or something like that. Professional liability, you don't want to be an additional insured, right? Because then you would have no coverage. But I tell my clients, and I've preached this for over a decade, is do not allow a third party to have access to your most valuable asset. Because you want to be able to, if you have a limited...policy limit, you wouldn't be able to direct those funds to keeping your operations up and running as well as indemnifying your client, right? You don't want your client stepping in and taking up all your limit.

So I personally, I always redline, you know, if they say we want additional insureds under all policies required by this contract, I say, except for technology errors and omissions. And 90 % of the time, I don't really think the other party on the other side knows what they're asking for and it just goes through. When they do push back, we then discuss why on a technology professional errors and omissions policy, you do not want to be an additional insured. Let our client direct funds and take control of the legal process. And they generally subside. They usually say, okay, we get it. Larger, really sophisticated companies push back pretty hard sometimes. But my general advice is anytime that you can keep a third party from accessing your tech E&O or cyber policy as an additional insured, redline that when you can and you'll protect your policy, your guidance of funds, you know, as you as an organization. So I highly recommend no additional insured for tech E&O.

[Kevin]: Well, that's great advice. And I think that's a great place to leave it. So let's pause for now. Damion, I really appreciate you stopping by Cyber Sip. I think this has been a wonderful and invaluable conversation for our listeners.

[Damion]: Great, well thank you for having me. It's a newer product compared to most lines of insurance, but I think most people have gotten more adapted to over the years. Seek out a professional broker, seek out counsel that understands the coverage, and then as an insured or as a legal counsel, I think you're in good shape.

[Kevin]: You said it well. Damion Walker, thank you so much for joining us on Cyber Sip and thanks to all of you for joining us. We're back soon with another episode.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, and Spotify. Like, follow, share, and continue to listen.