# *Barclay Damon Live* Presents *Cyber Sip*™
# Season 4, Episode 2: "Navigating the Cyber Insurance Landscape: Trends to Watch," With Kelly Geary

Host: Kevin Szczepanski, Barclay Damon

**[Kevin Szczepanski]:** Welcome back to *Cyber Sip*. And welcome back to you, Kelly. I think that this is your third appearance. So we need to do one of those SNL skits where surprise guests come out and take the stage to honor this...

**[Kelly Geary]:** I would love to do that with you, Kevin. Any time.

**[Kevin]:** We won't do it now. But I should introduce you for the three or four people that don't know. Kelly Geary's a managing principal with Epic Insurance Brokers & Consultants. She is also the national practice leader of the Professional Executive & Cyber Solutions Group, and she is one of the few people that I turn to when I don't understand something. And hopefully that doesn't happen too often. Welcome back to Cyber Sip, Kelly. Thank you so much.

**[Kelly]:** Thank you for having me, Kevin. I love it.

**[Kevin]:** So, I sent you some...a list of topics before we got started. I'm going to start with the most generic one because I can't wait to hear the answer. So what keeps Kelly Geary up at night in your role at Epic as we ring in 2025?

**[Kelly]:** Oh, it's such a good question. So many things keep me up at night. I would say, the key thing that I thought of when I looked at that question was, the cyber market, and, you know, whether or not it's going to turn, you know, right now we're in a very soft market. It is definitively a buyer's market right now. Notwithstanding the continued, you know, escalation of cyber-crime and ransomware attacks and, you know, systemic attacks like Change Healthcare. And so, you know, we love that it is a buyer's market. We love that it is a soft market for cyber right now. But just wondering, you know, just hoping it stays that way. For our clients, and for insurance buyers out there.

**[Kevin]:** I noticed in some of the great Epic materials that you put out for all of us to read, it sort of stands alone. I think that, it looks like cyber and to some degree, DNO, you know, are both flat to softening. But every other seems like every other category of insurance is up. The market is hardening. Why do you think that... we'll focus on cyber...why do you think the cyber market stands out as a softening category?

**[Kelly]:** I just think there's a lot of capacity. I think that, you know, when we went through the hard market, two years ago, I guess it was, 2020 to 2022, roughly. I think, you know, there was a significant change in the way that, markets were underwriting the risk. It was a much more detailed, deep sort of dive into cybersecurity and data privacy. And I think that that, created a much more, welcoming environment for some markets and other MGAs that were out there considering whether or not to get into cyber or really, jump into cyber. And I think that with that sort of increased rate, that came during the hard market and then the sort of

change and shift on the underwriting side, it made it a little bit more palatable to a lot of, a lot of companies. So we have a lot of capacity out there right now.

**[Kevin]:** I know we're going to talk about this in a bit, but I want to follow up on that. Are you saying that in some sense—and I may have this wrong—in some sense, the tightening of security controls and the tightening of the underwriting was one way that the industry actually improved the insurability of cyber risks, thereby bringing new insurance players into the market? Did that actually happen?

**[Kelly]:** I think that that is definitely part of it, right? I mean, I think, prior to the hard market, you know, the underwriting, the approach to underwriting was, very, very cursory. You know, you could get yourself a quote from a lot of markets based on three or four pieces of information. And, and it wasn't really a deep dive. And I think that one of the key elements that we saw pushed during the hard market really was MFA. You know, during that period of time, if you didn't have MFA to some extent, at some level, you weren't insurable at all. And, and interestingly, now as we move into the soft market, there's less of a focus on MFA. I mean, it's still I think it's still pushed businesses to push... to put MFA in place. But, you know, not necessarily across the board and not necessarily in all industries and in all size, companies. So it's kind of interesting where we're at now.

**[Kevin]:** Yeah, that is interesting. So progress is not a straight line. It's zigs and zags. All right. So let's dive right in. What cybersecurity trends should we be watching out for? Are you watching out for the coming 12 months?

**[Kelly]:** Well, you know, I hate to say AI because I feel like everybody says AI. But I don't think you can avoid, you know, talking about AI and generative AI when you talk about cybersecurity trends, I think that there are tons of positive things that are happening with artificial intelligence and generative artificial intelligence in terms of defending, helping defend networks, against breaches and attacks and that sort of thing. I think that AI is probably, you know ...attackers are probably getting more out of AI than defenders, just because there are less parameters around it. Right? I mean, I think that we, we as, organizations and as a society are trying to sort of put guardrails around our use of AI in some way. Whether it's legal guardrails or ethical or just guidelines in general. Right. As we implement and start to utilize AI, I think that obviously attackers and cyber criminals don't have those guardrails. So they can use it to its fullest extent for bad. Right. Whereas our ability to use it to help us defend against those attacks, although it is... we are being able to use it. It's harder for us to get there.

**[Kevin]:** Do you see...So sort of thinking about that, just thinking about, our discussion I think last year at this time, we were talking about whether the expectation was that an organization have a full-on AI policy, should it at least be an AI position statement. Something that's disseminated to the employees of an organization? Have you evolved in your thinking on that? Where does that stand from your perspective?

**[Kelly]:** I yeah, I still think you need you need to have some sort of position. I still will stand by my point on, you know, if you put a policy in place, you better be ready to actually follow that policy and update that policy. Because in a litigation setting, if you have a policy and you know, somebody is able to show that you didn't follow that policy, it's... you're in a worse off position than if you didn't have the policy at all. So you definitely have to have some sort of position on the use of AI...I think most companies today do, but I think that one of the things that comes out of that and is sort of rearing its head right now, because we went through a period of the last, you know, say 18 months of companies rushing to implement some sort of guideline or position or policy on AI and, you know, kind of employee it's use of it. You have this, evolution of shadow AI where you have people at organizations that are going outside the guidelines set by the organization, and utilizing ChatGPT at home or in some other fashion or some other, you know, form of AI model and then bringing it back into the workplace and still using it outside of the scope of, the organization's policy or position or guardrails. And so that I'm wondering what that will look like as we move forward and what problems.

**[Kevin]:** Yeah. I wonder and I, I want to talk a little bit about claims and coverage issues. And I wonder, as you were mentioning, that I was thinking if the industry does eventually start implementing AI-related endorsements or exclusions across the board, could that maybe be one area where you would see an exclusion... is you could fairly tightly identify it. And the exclusion is for AI that is, I don't know, AI that is used outside the scope of the organization's policy procedures or AI that is used on a personal device. It strikes me as... that doesn't sound quite right to me, but I wonder, have you when we talked last year at this time, you know, people were asking, is there going to be AI coverage? Will there be AI exclusions? Has the market evolved to a place where carriers are starting to get their arms around what those endorsements might look like?

**[Kelly]:** A little bit. You know, we have seen some endorsements specific to AI. We've seen some outright exclusions. I actually I think I saw an outright exclusion on the lawyers' policy. Lawyers' professional liability policy ...

**[Kevin]:** For research?

**[Kelly]:** It was very broadly drafted, just across the board. Which is interesting. Right?

**[Kevin]:** It is.

**[Kelly]:** And we've seen some other, attempts at trying to exclude or preclude or limit coverage around the use of generative AI specifically. We've seen some, standalone products come out. We've seen a lot of questions from the underwriters, about, you know, do you have a policy, do you have a position? How are you using generative AI? And that's true on the cyber side and also on the DNO side, questions around that.

**[Kevin]:** It's an interesting question because... I think some people see AI as the end to itself, but I don't necessarily see it that way. I think that AI is just the means to the ends that organizations like law firms have been doing for years. So in that sense, I thought it'd be kind of difficult to put coverage guardrails around the use of AI, because after all, lawyers have to research and write like many other organizations, and we should encourage them to use state-of-the-art technology that makes that more efficient and cost effective for customers. So can I ask what, when your law firm clients come to you and say, hey, how do we get our arms around this? What should we be thinking about? What kinds of points do you make with them? What do you bring to their attention that you think might be helpful?

**[Kelly]:** I think you're starting to see some of the bar associations come out with some guidance, around the use of AI or generative AI in in the performance of legal services. And, and I think that, you know, from an insurance carrier standpoint, you know, in a product standpoint at the insurance product, it is hard to create, either affirmative coverage around the use of AI or restrict the coverage because it evolves so quickly, too. Right? And that's part of the problem. And there aren't really any regulations around it. And, not to any great extent. Right. We don't have any federal... we have the EU AI act, and we have some smattering of, of different state laws. But we don't have anything definitive yet. And I think that, you know, just in my own experience on the carrier side, drafting policy language, and applying it, it's hard, you know, especially liability policies. They tend to follow the law. And when we don't have a law, it's hard for a policy to put anything into a policy around it. Yeah.

**[Kevin]:** No, no. Agreed. That's true. There is no law. And the law there is deals with use of AI in HR, hiring decisions, or deepfakes, the sort of thing that I mean, it exists, certainly, and it can be problematic, but that may not be relevant to a whole host of organizations who may get into trouble for other AI-related reasons. When you... as you talk to policyholders, I actually am curious your take on this. So on one hand, I think we're all in a rush to implement AI because it's so exciting and we think we should. But on the other hand, it's a tool like anything else. And it seems to me that as an organization, I ought to be thinking about what do

I do? Could AI make me more efficient? What AI tool should I purchase or implement? And then what are the safeguards that I'm going to place around that to protect my customers, my employees, my data? Are we there yet in terms of thinking about it? Or and maybe these are just two extremes. Are we on the other extreme where we just got a lot of people rushing to use this exciting new toy without really thinking about how it helps or hurts the business?

**[Kelly]:** I think you have a little bit of both out there, right? I... you definitely have that sort of FOMO going on, that fear of missing out. Right? You have a lot of companies that are, to your point, rushing to implement various different types of AI for fear of being left behind in their industry vertical. Right. Or, you know, look, if we don't do this, these other five companies, I know they're doing it. They're right. You know, we'll get left behind. We'll lose clients. We'll lose customers. So there's definitively that rush, and I think that that's what tends to cause the most ...the problems, right, is when you're rushing to do anything, you know, whether it's you're in as an, as an individual, as a person rushing to do something, you're going to make more mistakes when you're rushing. Right. And I think that that's what, the real challenge for businesses is, is to really think very clearly about, to your point, you know, how can we use this to best improve our efficiency? And, you know, how do we do this safely? And to protect, again, from a network security standpoint, a data privacy standpoint. But you have a lot of companies that have service providers say, for example, a law firm or an accounting firm or an insurance broker, that are pushing their service providers to tell them how they're utilizing it. How are you making this? And so that push too, creates strain and pressure on organizations, and professional service fronts, certainly to, to sort of do something. Right. And then you have on the other side of things, you know, you have the companies that are making representations about how they're utilizing gen AI and AI that may not be truthful, or fully truthful I guess. you know, and maybe deceiving. Right. That's the AI washing, I think.

**[Kevin]:** I think too, it's just getting back to basics is going to be so important for us. I was just looking at an AI contract over the weekend, and, what troubled me about the contract were not the provisions relating to the use of AI. It was just the good old fashioned indemnification insurance procurement provisions. And they were badly drafted and fairly weak. And these are provisions that are in the AI vendor's form contract. So I think one piece of advice that if I were put on the spot, I think I would say is, look, I know you're dealing with AI, but that's just the shiny new toy. That's just the name. Be sure that you deal with the basics like risk transfer and coverage for the risk transfer. And I think one of the dangers is that everybody's in a rush to implement, and they may sign a document that they wouldn't have signed five years ago because would have recognized all of these weaknesses.

**[Kelly]:** I think that's a great point. I think that's, you know, there are so many vendors out there pushing products and services that are AI-powered, right? Or AI assisted, that businesses are trying to sort of, you know, to your point, just, you know, sign on to anybody without even perhaps even vetting the business. These are a lot of startups, right? A lot of businesses that really haven't been around for very long and are just trying to get in on it. Right. And so that that can be problematic for companies as well. Forget about the contract piece of it. But, just vetting the vendor. Yeah. Product.

**[Kevin]:** Yes. Oh, and that's a whole other ...that's a whole other episode too. You if, if you were held, if you're an organization that's held to a regulatory standard and you have a vendor that you haven't vetted to see whether that vendor complies with the regulatory standard, then there's an argument that you're out of compliance. And we're... I think sooner or later the regulators are going to pay more attention. And we're going to get busier. But let's stay on AI for a minute. So the claims I'm most familiar with and interested in are the claims against lawyers for misusing AI to conduct research and draft motion papers, citing case law that doesn't exist. And that was a big deal a year ago. What's your experience... from your claims lens? What does it look like out there? Are we seeing more of those claims? Are there other types of cyber or AI claims that are occurring with more frequency?

**[Kelly]:** I think I would say that the most the most significant trend, I guess from my perspective, is an increase in social engineering fraud with deepfake audio-video. And so that's basically AI-assisted, social engineering fraud. I'd say that's what I've seen the most recently. And, you know, it just makes the attack, much more profitable and successful for the cybercriminal. And much, much more difficult for the victim-company to be able to identify and prevent.

**[Kevin]:** What do you... so what are the flaws that you see in these claims that the companies might have eliminated if they were a little more careful or a trained a bit better before the event occurred?

**[Kelly]:** It's honestly it's hard. It's hard to say. I think that we need to try to figure out how to better detect deepfake audio-video and then train our employee base pretty frequently because, again, it goes back to the challenge that the technology evolves very, very rapidly. And the cybercriminals have an incredible financial motivation to be very good at what they do. Right. And to improve their skill and improve their profitability and their efficiency at perpetrating these attacks. And they're doing a great job.

**[Kevin]:** Yes. Yeah. And I think, I don't know that there's any way around it, but I think we're going to have to look at organizational policies that say, you know, if you get a call from the CEO asking you to transfer X amount of funds on, you know, ...by a certain time frame, you're to hang up and call the CEO using trusted contact information and verify that. And your CEO will want you to do that. I don't know how we get around having those policies in place, because there is so much pressure in everyday organizations. And when you think you've gotten a call or a video, you're online with your CEO or CFO and he's asking you to make an emergency transfer, it's really hard to say "no." But on the flip side, how often does that actually happen? It's happening. The threat actors are employing it.

**[Kelly]:** Yes, yes.

**[Kevin]:** How often does how often? I can tell you that my CEO, my managing partner, has never called me on a rush basis asking me to do anything resembling transferring funds.

**[Kelly]:** Yeah. No. Me neither. But one of the things that I that I have seen, or I'm starting to see, organizations employ to try to deal with this is, the use of a code word that is changed on a regular basis. You know, to try to help organizations or people in an accounting department or somebody that actually is in charge of moving money. So, so that they can ensure that they are talking to the right person. And that, I mean, that's one way of approaching it. I think, is... that's pretty good. We'll see if it's sustainable. You know, if you put the code word out on your network, though, you know, could the, you know, I mean, how do you get the code word, how do you dispense it? How do you update it to make it... in a way that is not network-based in some sense. Right.

**[Kevin]:** No. And there probably ways to do it. And maybe some of them are going back to basics and just communicating offline, communicating that sort of thing for offline. You mentioned training. So we've got a few minutes left. I want to ask you about that. I have been and I won't mention names, but I because I don't mean to disparage this online training service. We use it here at Barclay Damon, but I know you folks at Epic have been doing some really careful thinking about the importance of employee training. And there's some, at least, if not empirical, at least, and anecdotal evidence that these training services are not as effective as we think they are because people are doing them independently. They may not be watching the instruction consecutively, and they may not be getting as much as we all think they should be getting out of the online training. Have you encountered this and what, if any, solutions are the folks at Epic devising to try to make training more beneficial to the folks in the trenches?

**[Kelly]:** It's such a great point, Kevin. I think, you know, we all have trainings, right, that we have to do as a part of organizations. And I think, myself included, we're all guilty of sitting there and multitasking. Right. Well, while you're doing the training, you're like, oh, I have to do this training before, you know, January 1st and

you are doing 15 other things and you have it on in the background. Right? And, and we all understand that. I think with cybersecurity and data privacy, it's just so difficult to really effectively educate your employee base. For that reason, because all of these sort of standard trainings are going to result in that type of scenario, right? You know, some of the things that I've seen organizations do that I that are sort of new and, interesting is more immersive trainings where you actually are, you know, now that we're back, in offices and all of that good stuff, you know, mandating, in-person type trainings that are more tailored to certain groups or levels of employees. And in smaller groups. You know, when you and I and I understand certainly that if you're an organization of 5,000 employees, it's very, very hard to do, but maybe you do it on a, on a regional basis, on an office basis. Where you kind of try to do that. I honestly, I think it's...you have to customize the training and, and it has to be pretty frequent. You know, I've seen, trainings, just in the underwriting process when I review underwriting apps, some of the trainings that have come through and I look through them and they're, you know, from five years ago, and, you know, the regulatory environment is very different today. The threat environment is very different today. And you might be able to do that with, you know, sexual harassment training and, and discriminate... You know, you can do those kinds of trainings where with those topics where they're sort of "set it and forget it." And you can use it for a number of years. But with cybersecurity and data privacy, it's different. It's got to be very, very flexible and nimble.

**[Kevin]:** That's a good point. I think you're right. I think the employment discrimination videos are... there's a consistency over time. There are changes based on sex and gender differences and evolutions in our society. But for the most part, the content is the same. I remember... I think it's Jim Dempsey who's a noted national cybersecurity expert, literally wrote one of the books on cybersecurity. And when they came back to him, I think it was 18 months after his book was published, he had to he had to supplement it because so much had changed in that period of time. So, no, you're absolutely right. We are running out of time. So how do I... how do we end this episode? All right. I know you are always flawlessly prepared, but

**[Kelly]:** Thank you.

**[Kevin]:** I'm going to pretend that we're in an elevator. That's that'll be the fiction. And you have one opportunity to give an organization your best advice. This is if I tell you this, you will be 50% better protected or more insured and maybe overstating it. It's my fault. What do you say to that organization? What's the best opportunity to get someone's attention and really take the next step in their cyber hygiene and insurability?

**[Kelly]:** I would say truthfully, is tabletop exercises, holistic tabletop exercises. A lot of organizations say they do them, and many do. But the ones that I've seen, they're not frequent. You know, they'll do them annually and it sort of goes back to the training comment, where you say, you know, people are half engaged. I would say really take that seriously. Do them frequently, have conversations about, you know, whether or not you would pay a ransom very frequently, you know, be prepared because it will happen. And the tabletops are really probably the best way to get your entire organization ready.

**[Kevin]:** Yeah, I think that's absolutely right. And one thing I would add to that is if you're doing it, make it as realistic as possible and expect to fail. In a good tabletop exercise, you should fail because unless you're pushed to the breaking point, you're not really going to know where you need to improve. Every organization fails just, you know, don't fail in the first five minutes.

**[Kelly]:** Exactly!

**[Kevin]:** Well, Kelly, thank you so much. I know how busy you are, and I'm really grateful for your stopping by for your third appearance on Cyber Sip. I always enjoy our conversations.

**[Kelly]:** Thank you so much, Kevin. I love being here.

**[Kevin]:** And I look forward to seeing you again soon and to seeing all of you soon on our next episode of *Cyber Sip*.

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