Barclay Damon Live Presents *Cyber Sip*™
Episode 38: "2023 Trends in Cybersecurity Claims and Coverage," With John Farley

Speakers: **Kevin Szczepanski**, Barclay Damon, and **John Farley,** Gallagher Insurance

[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]: John Farley is managing director, US cyber practice for Gallagher Insurance, which is now, John, if I'm not mistaken, the number three insurance broker in the country. And he joins us today to talk about where we are and where we're headed in the world of cyber and cyber liability coverage. John, welcome.

[John Farley]: Well, thanks, Kevin. My pleasure to be here.

[Kevin]: So glad to have you. And with someone like you, one of the first questions I want to ask is, you know, we're sitting here, we're through the first quarter of 2023. I can't believe we are, but that's where we are. And what trends are you noticing in 2023 that are a little bit different perhaps from last year?

[John]: Yeah, well, maybe we could start with claims, right? That's really kind of where the rubber hits the road, and that's kind of what drives the market. So, you know, what we saw last year, especially towards the end of last year, was a trend downward in terms of ransomware, severity, and frequency. So that was a great sign. We were hoping for the same as we went into 2023. But unfortunately, as the cyber market and cyber threats typically do, they surprise us, right? It changes. And sure enough, we're seeing an upward trend in terms of number of ransomware attacks. And I talked to breach coaches and I talked to incident response providers on a regular basis. And almost universally they're indicating that they're seeing that upward trend again. So that's unfortunate because we were hoping to continue that trend downward.

[Kevin]: Right. Now I was taking a look at Gallagher's... And this is your... the 2023 US Cyber Market Conditions Outlook Report. And with regard to ransomware, I think there was some thought at least earlier this year that one of the reasons it was trending downward was the Russia/Ukraine war was diverting the attention of hackers that might otherwise be deploying ransomware to other places. Do you think that's one of the reasons why it trended down last year? And are they... do we know whether they're now refocusing their efforts on the West in 2023?

[John]: Yeah, well, I would definitely believe that, at least in part, some of the trend downward last year was due to that. Exactly that. They were distracted with a real, you know, real hot war, if you will. Right. Dropping bombs and deploying resources there. That was one of the reasons. But I also think a lot of the work that we as an industry put in underwriting controls that were mandated. You know, if you didn't have MFA, there was a chance you're probably not going to get even a quote. So those controls were forced upon those that were applying for cyber insurance and renewing their coverage if they didn't have them in place, you were non-renewed. And then the carrier really had just a better book of business in terms of cyber control. So they fended off attacks, I think. And I think those that came through were mitigated in a way that they weren't before. So, you know, I like to kind of give kudos to the industry for the work they put in. I don't think enough credit is given to the industry as a whole and to the clients that pivoted as they could and deployed resources

to prevent these type of attacks. So a lot of work went into and I think that also was part of driving the trend down. But of course, you know, hackers evolve as we know. They always do, and they try to figure out ways around your defenses. And perhaps that's happening at least to some degree now. All that said, I mean, I don't think there's any indication that we're back to where we were in 2020 or 2021, where, you know, carriers are paying, you know, limit losses on a regular basis. I think we're going to sort of wait and see here and continue to, you know, implement those controls and figure out the best way to stay one step ahead of those hackers. It's really... it's a race with no end, as they say. Right. There's no finish line here. There's a constant battle.

[Kevin]: Agreed. No, that's a great point, John. And I think that one of the things that always troubles me about ransomware is, is the existential threat to an organization. When your system is down, you literally can't do business and you can't restore your business from backups. So it's good to hear that trend is down, maybe coming back a bit in 2023. But is ransomware the chief issue that you're seeing now? What about business email compromise and some of the other cyber threats? How do they play into the threat landscape this year?

[John]: Yeah, you know, it's funny, they kind of hadn't made the headlines—business email compromise and sort of funds transfer fraud type claims—but if you look at the FBI report that comes out every February, the one that came out this quarter, that indicated that those type of attacks stayed steady, they're continuing and they're hitting the bottom line really hard. So we... really we're still struggling with that. And I think it's getting more and more difficult. There's a lot of new techniques that hackers are using; deepfake technology, right. ChatGPT that, you know, they're using different means that kind of craft phishing emails that may not have misspellings. Right. And, you know, easily seen. That was always a telling sign. You could say. All right. There's misspellings here. Poor grammar. This looks like a phishing email. Well, what we can see, they're going to start to leverage new technology like ChatGPT to kind of craft these realistic looking phishing emails. So we're really concerned about that. And we're trying to take steps to educate the workforce of our clients, every single person about these kind of attack techniques so they can spot them.

[Kevin]: Right. Yes. I don't know what hope we have if the email you get from me sounds like me and that's what AI can do, right? We've got to have another episode. I think AI...there's a lot of extreme talk around AI. Maybe we'll come back and talk some time. I think we're going to have a guest on later this year. I think there's a lot of justified concern and a lot of unjustified concern. But with respect to business email compromise, that's going to make it a lot different and a lot harder for good folks to try to prevent those attacks. Yeah.

[John]: Yeah, absolutely.

[Kevin]: Yeah. Okay. So I have to ask you this. It was the subject of one of your webinars earlier this year, and I wanted to have you on to talk about it. A certain CEO to go unnamed said last December something to the effect that cyber risks will eventually become uninsurable. I want to ask you about that and get your reaction to that and maybe speculate a little bit about what this CEO might really have meant when he was saying that if he didn't mean literally that the risks would become uninsurable. What's your take on that?

[John]: Yeah, I mean, I don't know that I can comment on how what he meant or what he was trying to convey if it wasn't exactly what he said. But I will tell you, it absolutely is insurable. And there's evidence of that based on what happened last year, how this market sort of stabilized, how we got a lot more mature in how we approach it and how we underwrite for it as an industry. And carriers became profitable. You know, they went through a rough patch there in 2020, 2021 where they made the loss ratios were not good, but they, they improved drastically. So I mean, I would argue that that we've demonstrated that it is insurable. It's something, though, that, you know, we have to keep our eyes on. We have to understand and try to get a better grasp on systemic risk. Is that a possibility? And if that does occur, will all the policies respond? And what... that language is changing kind of on a daily basis, right, from carrier to carrier. So we're still sort of in a maturing phase right now, but I believe we're taking steps to make sure it's stable and sustainable. But I

think, you know, we've seen evidence of, you know, reinsurers really taking the spotlight here to making sure that, you know, the books of business of any particular carrier, you know, they're looking out for that systemic exposure and they're taking steps for backstops like we're seeing insurance-linked securities now entering into the picture. Right. We saw Beazley came out with a cat bond [Note: catastrophe bond] where you have backing of, you know, the private sector really backing the carriers here. So we have a cat bond set up to back them $45 million. So that was a great first step. So I think, you know, I would argue that this is a market that's maturing. I'm seeing more steps taking taken to allow for more capacity. Right. So we can have more growth. I'm a bit of an optimist by nature so ...

[Kevin]: Me too. Me too.

[John]: Yeah. So I mean I'll take a different opinion there and I haven't seen anything that's indicating that this is going to shrink in any way. I think this market is competitive again and growing. And again, but that, you know, this is the systemic risk that that we're concerned about is real. I mean, I do think about it almost on a daily basis. And I think our underwriters are thinking about it as much. And I think we just have to get our arms around it, trying to quantify it, figure out how the policies are going to respond and make sure that we're sort of sustaining this as we go forward.

[Kevin]: No, that makes sense to me. And you're right not to speculate about the CEO's comment. I don't know why I'm hiding it. It's the CEO of Zurich Insurance, Mr. Greco, made those comments back in December. And I guess I thought, trying to put a positive spin on it, it was in some sense a call to arms. We all need to realize there is systemic risk. It's only going to increase. And if we don't undertake certain safeguards and protect ourselves as an industry, eventually that risk is going to swallow the entire industry whole. So maybe that's what he meant. But I have a question for you: In order for the market to remain stable and to increase capacity, things can't stand the way they are now. They'll continue to evolve. Insurers will continue to require increased safeguards. They may also raise premiums and reduce limits to reflect a particular policyholder's risk. Talk to us about how carriers are looking at those security controls and what they're looking for when they underwrite policyholders in 2023.

[John]: Sure. You know, they're looking at a number of controls and we preach this all day to our clients. First of all, multi-factor authentication is clearly something that they have to have. If they don't have that, we really have to have a different discussion before you get in front of an underwriter. Right. So we're looking at that. We're looking at endpoint detection and response, right? So using artificial intelligence to tell you the second that the bad guys get in, all too often, we're seeing, you know, the hackers getting in and not being discovered for weeks and sometimes months on end.

[Kevin]: Right.

[John]: And by that time, they move laterally around the organization and they've exfiltrated data. And then, you know, just, you know, had that really had their way with a particular victim. And so that's something that we're seeing almost mandated now. We're also having other controls mandated, including patch management. So when a zero day vulnerability comes to light, the underwriter does want to hear that, you know, you don't know how to patch that for 30 days. Right. They want to see evidence that you have a program that can patch that vulnerability almost immediately. Right. And so...

[Kevin]: Right, right.

[John]: So being able to respond quickly to the threat, I think the underwriters know, we're going to be attacked over and over again. It's a question of can you respond quickly? Can you patch those? And then, you know, how do you mitigate it, right? I mean, do you have that backup right, when there's a ransomware attack? And is it air-gapped from your primary data set so the hacker can hop to that and encrypt that data, too, and

then they're going to ask you questions about, you know, have you tested the backup and how long does it take you to get it up and running? Right. It's not 30 days, right? Because by that time you've got a business interruption loss that's probably going to lead up to the policy limit. So there's a lot more questions around controls like that. And, you know, those applications can get pretty involved. But our job as a broker is to get our clients prepared for those questions. You know, we see it all day, every day. And so we're just trying to... as question sets change. They may get longer, sometimes they get shorter. We'll make sure our clients are prepared as to what they're going to be asked.

[Kevin]: So, John, you mentioned earlier the leading role that the industry plays in encouraging cyber hygiene on the part of businesses across the country. And I'm not sure if the industry plays an equal role in... with respect to every risk, but it certainly seems to be playing that role with respect to cyber risks. Can you talk a little bit about that? Do you agree or am I just imagining things?

[John]: No 100%. And it's not just because I'm a broker in cyber insurance. I see, you know, every day carriers coming out with policies and adding more and more cyber risk services that come with the policy. Right. So if you are a policyholder, there's a very good chance you're getting perhaps free or discounted services to help you prevent or mitigate a cyber-attack. And they come in the form of phishing training. They come in the form of scanning services, incident response planning, tabletop exercises, even help with compliance to privacy law. So, you know, they're in the game here, right, the carriers don't want to have a claim. Of course, our clients don't want to be attacked. And if an attack happens, they want to be able to prevent further harm, both financially and reputationally. So these are services that, you know, weren't always taken up in the past. Right. But as you know, we saw frequency and severity tick up a couple years ago. We start to get a lot more attention on these services and more carriers offered more of them. And so it's been a really healthy exercise where these are offered and taken up and clients are then more prepared for the attacks. And so overall that's helped us become more mature in ways to defend and mitigate attacks. So these services are so important. You know, we ...when we have a new client and we onboard that a client, one of the first things we talk about are these services depending on the carrier you're with to make sure they're aware of them. I mean, some clients are already doing phishing training and that's great, but maybe additional services can be provided to really round out the cyber risk management program of that particular client. And those services are one way to do it.

[Kevin]: Absolutely, John. I think, and folks oh, sorry, we had a little lag on our end. But no, I agree completely. And I'll tell you folks, if you've got a free tabletop exercise as part of your insurance policy, do it. It is the next big thing. Everyone's going to be doing it. Eventually, carriers are going to be asking you whether you do them. You sit in a room with all the stakeholders in your organization. You run a mock incident response, you communicate with all the stakeholders. You learn about your strengths and your weaknesses. And most importantly, you ensure that when the inevitable incident happens, be it a ransomware attack or business email compromise, you are not responding for the first time. Practice makes perfect, and a tabletop exercise ensures that you have practiced for that incident response right?

[John]: Absolutely. Yep. Practice makes perfect, as they say. Not that every response is going to be perfect...

[Kevin]: So, John, I want to close. Yeah, right. It's so funny you say that because I use these old aphorisms with my teenage children and they've never heard them before. So you say "practice makes perfect" and they look at you like what? I've never heard that. But I want to be respectful of your time. We're coming to the close, but I want to ask you about some of the key players that you wrote about that you believe will be shaping the 2023 cyber insurance market. And you have several listed, but I'm going to focus on just two. First, reinsurers and second, government regulators. So, how will reinsurers be shaping the market this year in a way that they may not have shaped the market in years past?

[John]: Yeah, I mean, I think a lot of people don't realize that, you know, a good portion of premiums that the primary carriers take in, they cede to reinsurers. Right. And so reinsurers are going to play a very big part

in terms of providing capacity. Without reinsurers, you won't have the capacity for the market to grow and they've got to get comfortable with the underwriting processes of those primary underwriters and the risks they're taking on and what those policies are covering and what they're not covering. So we're seeing evidence now of, you know, they're really taking the spotlight, right? They're the ones that we're all looking to. Just a couple of years ago, you know, we weren't even talking about, you know, reinsurance, right. But as the market hardened, the capacity was cut. And now we're looking at, you know, how do we increase that? And that's one way to do it. So we're bringing in insurance-linked securities too, to backed reinsurance. So there's really a chain of folks involved here who will play a part. So as we see those kind of investments come in, it's really exciting to see. It's really going to be the key to growth. And as we get more capacity, you know, we'll be able to get those policy limits that our clients really want. Sometimes, you know, especially in the harder market, we couldn't get policy limits and our clients wanted it, but the carriers were not willing to give it. I think we're going to hopefully move the other way now and really grow the market.

[Kevin]: So we talk about reinsurers and my guess is that as reinsurers look under the hoods of the primary cyber insurers, those insurers in turn, are going to be increasingly focused on security controls that will impact policyholders. So it all kind of rolls downhill, some, so to speak.

[John]: Absolutely. Yeah. It's one, you know, sort of chain there. And everybody has an interest in preventing attacks and mitigate them and underwriting controls for sure.

[Kevin]: So I want to close with you on the impact that government will have this year and in the years to come. It seemed to me that in past years the government was focused on encouraging critical infrastructure companies to share information and discouraging companies from paying ransomware ransoms, but not much more than that. That has changed in the last year or two. We're seeing governments implement an increasing array of security controls, implementing increased governance requirements. What are you seeing on that horizon? And what do policyholders need to look for?

[John]: Yeah, yeah. I mean, I'll tell you, you know, at the state level, at the federal level and even in the international level, we're seeing privacy regimes, you know, really around the world having something to say about all of this. But one area that I've focused on is the concept of "wrongful data collection." Right. And what's happening, I think a lot of the at least at the state level in the US, we're seeing regulators saying, you know, the data subjects now should be given a lot more power. You and I have a lot more power on who can collect our data, who can share it, whether or not I have the right to have it you know, disposed of or changed. And so what's happening there? It's going from state to state. So California started it. There's a handful of states that have full comprehensive privacy laws now, but we're seeing a lot of legislation and probably a few dozen other states now looking to do something similar. So that creates a compliance issue, right? You may be collecting or an organization may be collecting private citizens' information, sharing it. It gets into biometrics, right? So they start expanding the definition of personally identifiable information. So we've seen a lot of BIPA claims now. So that really doesn't have a whole lot to do with hacking. Right. And Russia/China, it's about what you're collecting and what you're sharing. And as a result, you know, you could have not only a regulator all over you for an investigation and perhaps a fine or penalty, a lawsuit. Then the plaintiffs bar piles on and you're seeing class actions follow the regulatory investigation. So that's another whole aspect of cyber risk that I think is really starting to get some traction, and one, we have to keep our eyes on for sure.

[Kevin]: Yeah, I agree. No, good thoughts all. Right, John, I want to thank you so much for joining us. I know we're running up against our time, but it's great to talk to you. And I just have to tell you, there is... there are few people in this industry who are as calm, concise, and informative as you are when you speak. And I know you are a cyber evangelist, so you're always on the go, speaking to policy holders, lawyers, and other groups trying to spread the word about the importance of cyber hygiene.

[John]: Well, thank you for that, Kevin. You know, it's a labor of love. I love what I do and it takes a lot of work and it's a continual effort, but it's a fascinating world. And if we can make a difference to help our clients prevent or mitigate those types of attacks, I think, you know, we're doing our job, but it's going to it's going to continue to evolve. And I'm happy to take on the challenge.

[Kevin]: Well, we appreciate your joining us today. Thank you so much for joining us on Cyber Sip. And thank you for joining us. And we'll be back soon with another episode.

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

This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied. Thanks for listening.

Barclay Damon Live *podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of* Barclay Damon Live *programming is the audio file.*

Thanks for listening.