Barclay Damon Live Presents *Cyber Sip*™
Episode 32: "It's No Game: Maximizing Your Cyber Security Coverage," With Brandy Griffin

Speakers: **Kevin Szczepanski**, Barclay Damon, and **Brandy Griffin**, Crum & Forster

[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]: Welcome back, everyone. We have Brandy Griffin of Crum & Forster with us today. Brandy is senior manager, cyber incident response and e-risk. Brandy, gee, welcome to *Cyber Sip*.

[Brandy]: Thank you, Kevin. Great to be here. Appreciate you inviting me to the podcast.

[Kevin]: Oh, no, it's great to have you. So let's dive right in. What are the trends as we chart through 2023? We've always had ransomware and business email compromise. Is there anything new or any evolutions of those two risks that you're experiencing over at Crum & Forster?

[Brandy]: Sure. So some of the... I think the ECs are kind of remaining the same, right? You either have a transfer of funds or a breach of an account, right. Where someone has gained access to that account. So that can go one of two ways. But with ransomware, we're definitely seeing the threat actors evolve and kind of change their tactics. And I personally think a lot of that goes back to they know that people have really become more resilient with their backups. So where that was a weak point before, that is not necessarily the case today, which is a great thing for us. We need to keep moving forward with having those ransomware-resilient backups. So what we're seeing now is a few things. Black Cat is one threat actor group that has started saying, hey, if you don't pay this ransom by 5:00 on Friday, we're also going to launch a D-DOS, a distributed denial of service attack against you. Right. So that adds pressure to pay us. Obviously, there are laws now saying that you can't pay depending on where you're at, what type of you know, if you're a municipality, that may hinder you from paying a ransomware. But we're also seeing no malware ransomware demands. So no malware was deployed, but they have exfiltrated the data and they're saying we have your data and you have to pay. So that's interesting too again, they're like, we don't even need to deploy malware. We just need to take your data. And then on top of that, I will say that like cloud theft, same thing, right? Exfiltration of cloud data, demanding a ransom payment. And then too, one interesting claim I came across was the threat actor found the policy—this insurance policy policies—they had a tower...

[Kevin]: On this the network.

[Brandy]: ...on the networks they knew what they could demand. And so that was really interesting to see the negotiations with that threat actor because they were saying we know what you have available. We know what your deductible is. We know, you know, the ransomware coverage for the tower available [garbled] ever calls to you. And that's what we're demanding. So it's really interesting you know how we're seeing ransomware continue to evolve and now recent news ChatGPT. That is only going to help a lot of unsophisticated attackers create easy-to-deploy scripts. Ransomware as a service kind of created that, where you can go buy a script and deploy it. With instructions. Now it's only going to speed up the process. So a technology news need to keep evolving and watch it and grow with it.

[Kevin]: So the ransomware threat actors are going to begin using AI to their advantage.

[Brandy]: 100%. Yeah. And that's why, you know, we're really hoping that our technology moves as fast because everyone says AI, right. But AI's developing every day and becoming more sophisticated, so we need to keep an eye on that, keep moving with the ball, because they're only going to use it to their advantage.

[Kevin]: Now, the federal government has strongly discouraged the payment of ransoms. As you said, municipalities, many ways are not able to pay them. And it really is a moral hazard, right? Because if you pay a ransom, you're encouraging threat actors to conduct more ransomware attacks. What are you seeing, though, on your end? Are, is the payment of ransom going down? Is it going up? How have these public policies affected the typical policyholder when it comes to deciding whether or not to make a ransom payment?

[Brandy]: I will say from an industry perspective as a whole, based on some of the statistics I've seen, is that ransom payments have gone down. That's not necessarily a specific to Crum & Forster, but I don't really have the numbers on that for us internally. But as a whole, it has been seen that the numbers have gone down. And again, I think that goes to discouragement as well as just having good backups. Right, because you're going to deal with the fallout of data being access and exfiltrated no matter what. For the most part, from a legal perspective. But if you can avoid paying the ransom and come back up and deal with that legal fallout, the best that you can, I think people are trying to avoid paying this ransom to not fund these terrorist groups. And that's what they are.

[Kevin]: Oh, yeah, absolutely.

[Brandy]: Yeah.

[Kevin]: So let's pivot then, Brandy, and talk about what cyber carriers are looking for in the market today and what policyholders can do to maximize coverage. If someone came to you today and said, hey, what can I do to maximize the chances that I'm going to be able to get a Crum & Forster policy and get the coverage, or the most coverage that I could possibly get? How do you how do you talk about that policyholder?

[Brandy]: Sure. So I will say working with the underwriters has been super insightful for me. Now, in the insurance industry for about six months. So I've learned a lot. And, you know, our underwriters are truly risk management teams, right? They assess risk all day long. And so we kind of come in to assist them. We're another tool in their tool belt to kind of advise and dive in deeper when a more technical approach is necessary. So the things that I think a lot of carriers are looking for are, of course MFA, which should be standard for every account that you have.

[Kevin]: Talking about multi-factor authentication.

[Brandy]: Multi-factor authentication. Vulnerability management, endpoint detection and response and backups. As a whole, I will say this if a company is following some sort of framework such as CIS top18, nis CSF, NYDFS, is creating their own what seems like a framework for the financial services industry.

[Kevin]: Talking about the New York Department of Financial Services and some changes coming to the cybersecurity role when you're Part 500.

[Brandy]: It very much looks like a framework. It is right, outlining kind of a lot of the things that you see in NIS and CIS. And so while it is no easy feat for any organization to align with one of those, if you do, I think you can have more confidence going into the insurance process or even with, you know, customers saying, hey, you know, we're following this framework to a tee. We have governance in place. We don't just have tools, we have people, we have process, we have policies—we're auditing on a regular basis. And we're doing

all these things continuously. That will give you the confidence to go into any, you know, with the broker and underwriter to kind of have the conversation about your insurance and try to get the best coverage possible. The underwriters are always looking at the controls as a whole. It's not just one control. We often hear our insureds come to us and say, hey, you know, if I buy this tool that I'll get a lower rate on my insurance. And we'r like, unfortunately, that's not the case. It's not just one thing. It's a multitude of things. It's defense in depth. So we do look for multiple controls and we look that those are managed well as a whole.

[Kevin]: Yeah, let's talk about governance, because you mentioned that and it's not, strictly speaking, a security control, but you can think of it that way. So traditionally, I think most small- to medium-sized businesses assume that cyber security is the province of the IT person or the information security group and the chief information security officer. If you have one. The CISO is important, but talk a little bit about the trend towards placing the responsibility, the ultimate responsibility for data privacy and security in the hands of the organization's governing body, whether it's the board of directors or some other individuals.

[Brandy]: Sure. I think it's a complex issue, right, because a lot of organizations are still trying to figure that out. What ...who do they need? Are these internal teams that they're building? Are they relying on external resources to kind of help them manage that? We see it all the time on LinkedIn and other outlets that, you know, the board does take this seriously and it needs to be a top line issue. So I think it's going to be tough to navigate it because they need to make it a priority of their business. Do you have an Internet connection? You have a cyber risk. So you need to deal with that like any other business risk as a whole. Do your risk assessment, see what data is at risk? Right? How do we protect that data more so than anything else? How can we protect our network and any damages that could occur due to an attack. Really a lot of the regulatory things that are coming out of privacy laws are kind of trumping cyber security a little bit. They go hand in hand. There's a difference there between cyber and privacy, but those fines being levied are very hefty.

[Kevin]: They are.

[Brandy]: So I think, you know, keeping the data safe is one thing, but protecting the sensitive PII, PHI, any type of proprietary information, safe is really key because business corruption is one thing. But, you know, breach notifications is a whole other ball of wax.

[Kevin]: Right. And if there is business disruption, if there is disruption to the continuity of your business and you need to recover, that is something that the board needs to play a front and central role on.

[Brandy]: Absolutely.

[Kevin]: And many boards in small to medium size organizations may not have data privacy, data security expertise, but if they don't have them, what we're seeing increasingly is carriers and regulators saying, you have to go get some... you have to be advised by someone who does have that expertise so that you have all the information you need to make decisions on how to protect yourself.

[Brandy]: Yes. Yeah, absolutely. Like I said, it's not easy. It's a lot to navigate. I think what boards are dealing with is they hear all these acronyms that people throw at them. Right. And I think that the job of the CISO is really to try to look at it from a business perspective, not just technical jargon. So we hear all these terms, you know, EDR, XDR, SOAR, Sam, DCM, C, WPP naming off a few, and you can see how quickly those add up. And the board's kind of sitting there wondering, where do we start?

[Kevin]: That's a great point. And I was taking a note. I think we've got to do an episode in the near future on what questions a board should be asking. You don't want to get lost in the technical terms. You can literally drown in those, but you can avoid the technical terms. You can say, okay, what are our risks and what are the controls in place to protect them? And if somebody says, well, you need EDR, SIEM, I said, okay, let's stop. What are those and how do they work? And then when you get that explanation, you can say, all right,

are there any other controls that we haven't discussed that you think we should have in place? I think it's so important what you say, and I think it is possible and increasingly critical that we talk about cybersecurity, privacy, security controls in plain language.

[Brandy]: in business context.

[Kevin]: Yes, this is a.

[Brandy]: ...business issue, not a technical issue. Right. I, I kind of think sometimes back to you and I know you and I both have worked in e-discovery. Right. And so, you know, we know about the litigation preparedness that goes into that right. The EDRM, electronic discovery reference model, where you are governing. Right. What do you have? How do you preserve and how do you prepare for potential litigation? How do you prevent that in the first place? Right. And so I think using kind of that as the initial building block, right. We can build off of that to think about it from a cybersecurity perspective of how do we get ahead of this? What controls do we have, how do we lock down data? And just think ahead and thinking about, again, the technology is moving so fast, so we really have to keep up. And I think that's going to take, you know, your internal resources and externals. You just need to understand what people you have, who you have, and who you need. 'Cause technology alone won't save you. You can't flip a switch with the technology and walk away and think, you know, keep you from being attacked. You truly do need a holistic program with technology, people, and process. Yeah, let me actually say that over because it's people, process, technology from the start. Without that, it's going to fail. A lot of incidents I've worked on where because they've relied solely on the technology.

[Kevin]: Right. You're talking about and the concepts of, in some ways, the concepts of data inventory and risk assessment and those sound like, like big terms. And we're not sure what those things mean, but basically we're talking about what data do you have? Why do you have it? Who has access to it? Why do they have access to it? Is it ...

[Brandy]: Data retention? How are you getting rid of that data, that dark data that don't need any more? Right. If you can limit your exposure. You know, if a breach were to occur from 500,000 documents and people to half that, tha's a great thing right I can save you later. So it really is about the overall management and governance of whatever program you've put in place to kind of align with the best practices.

[Kevin]: We definitely need to do another episode on this. But if you have the board, if anyone in our audience has a board meeting this week or in the coming days to walk into a board meeting on either an agenda item or new business and just ask the question, hey, what data do we have and do we need it, and what are we doing to manage our data? Do we have a prudent document retention, document destruction, policy? Those would be great.

[Brandy]: Are we following it...

[Kevin]: Right.

[Brandy]: A lot of people have policies, and they're just not following it. And I was kind of a crazy person back in my day of e-discovery, you know, And you.

[Kevin]: You were not a crazy person.

[Brandy]: I was a crazy person in the way that I followed the data retention. It really bothered me if we had data that we didn't need. Right. And we never did because I stayed on top of it. We had a three-month retention policy to get rid of it. So I remember reaching out to the clients like, we have your data, what do you want to do with it? And really pushing for it and sometimes being to the point of annoying, but because I cared

so much about not having that data and making sure that that risk was kind of removed of our books. I really stayed on top of it. I think that's important to have people who are passionate, who truly do care to make sure that they're doing that part of the job really well, right? So you need the right people for the right job to stay on top of it. And you need different people. You know, you can't be a jack of all trades, master of none, right? So when you have a two-person IT team and you think that one person take care of my team, one person taking care security, both you know, both of those take a lot. So it's not realistic to think that that's possible. Which is why you may need to outsource a little bit. Right. To help those lean teams get things done.

[Kevin]: And understand the possibilities. You don't have to destroy the data. You can just take it off your system and archive it...

[Brandy]: Right. Yeah. There's yeah, like we would get different options. You know, we can, we can archive it, put it on a shelf, we can send it back or we can destroy it. And those are usually the options that you have available. But either way, you just don't want it online. You don't want it accessible to any threat actor. And of course there's physical access that you need to be concerned about. So making sure that that data is locked down, if it is sitting on a drive on a shelf somewhere. But you just have to think about it as a whole because there's so many risks out there. More so for Internet-connected devices. But the risk doesn't go away until you address it.

[Kevin]: Right? Right. All right. So I know you've got a schedule, so I want to turn... I've got two other questions I want to talk about with you. So let's turn to your role at Crum & Forster. And I know you're going to tell us about it, but I think it's really interesting. It is, in a way, bridging the gap between the underwriting side and the claim side. Can you talk us through that a little bit and explain why that's so important?

[Brandy]: Sure. So on the underwriting side, there are a few things that we do. When there is a more technical need to kind of discuss a control. You know, we want people to answer the questions on application accurately. So if it's a no, it's a no, but provide context so we can talk through it, it doesn't mean an automatic decline of insurance. It just means we need to discuss it and understand the risks. And so working with the underwriters has been has been really great in that sense to kind of, again, assess the risks as a whole and be a technical resource for the underwriter. We also do what we call cyber ready calls where we work with the broker three months prior to the renewal, we kind of tell them, hey, here's what we're looking for. That may change from last year.

[Kevin]: Right? Of course,

[Brandy]: It's a moving target. So we talk about the controls we're looking for. So they have time to kind of get those things in place to get the best possible coverage available based on, you know, the conversations of the broker and the underwriter. We also do onboarding calls, where we do a lot of preparation for... here's what an incident looks like, here's how to be prepared. You know, think about your contractual obligations. Here's how you'll be working with legal counsel like yourself, with IR firms. Maybe you need a PR firm. Maybe you need to hire ransomware negotiators, payment facilitators. If there is a notification requirement that legal counsel has identified, you may be working with data mining in breach of notification services. So we try to give them the whole picture because a lot of people have not experienced an incident. Just don't understand what all is involved. And that's normal, right? We deal with this every day in the industry, but a lot of folks are in this for the first time. So we just try to give them the whole picture and make sure they understand the process. And additionally, we do workshops and training for the underwriter. So that's the underwriting side that we assist with. We also, on the claim side, when there is a claim, we are working with the claims team to be on those calls. With the DFIR firm digital forensics in response, and the law firm, and just being again as a more technical resource to the claims team so that we can really make sure that our insured are getting exactly what they need. Everything is moving very efficiently and effectively and there are no hang-ups. And if there are, everything goes along the way. So we're to make sure that the insured is getting what they've paid for

their policy and they can trust that the vendors that are there are doing everything that they're supposed to be doing, and we're trying to get them back up and running as soon as possible.

[Kevin]: So important. Now, let me ask you this. How... is... do you encourage your policyholders to run their incident response plans before an incident? Talk to us a little bit about that, because I think... obviously you don't want to be running your incident response plan for the first time.

[Brandy]: Yeah.

[Kevin]: When you suffer a ransomware attack, you want to have some practice to build some muscle memory within your business. Can you share with us your thoughts on that? I think that's so important, but I'm not sure how many businesses actually do it.

[Brandy]: A lot of them don't do it enough. I agree. But I will say that's another thing that we do as well. We actually participate in tabletop exercises. We do IR plan reviews. So our team is, you know, can be at the table for that conversation. We are looking to see, hey, you know, let's take a look at your IR plan. Is it kind of outlining all the things that you would that we would expect? Because every IR plan is different. There are a lot of templates out there, but you want to look for kind of... are we touching base here? Do you have playbooks based on the type of attack that may occur? Right. A lot of organizations don't have those. Maybe some of the bigger ones, who are more sophisticated and have teams for that. But a lot of times you just have an IR plan and your plan is "call somebody." So there's a lot more to that. But my point being is a lot of times that's as basic as we've seen them. So we try to add more value there and highlight some of the things that they can be doing to prepare for that incident. We've also started... there's this really great card game called Backdoors and Breaches.

[Kevin]: You were telling me about that.

[Brandy]: Yeah.

[Kevin]: Tell our audience about it, too.

[Brandy]: It's an incident response card game. I totally recommend it. Go look at it. It's on Black Hills Security and it kind of runs you through scenario and it'll throw some random scenarios, right? And it's just like what an incident would do. So you never know. Every incident is different, but it really helps you to get thinking about the different types of incidents.
Gets you thinking strategically about what to look for during an incident, where to kind of point to during an investigation. And we can situate it in a way that's not just technical people. It can be for risk management folks like yourself who are lawyers in the space who you see this and you know, and you hear what's going on during an investigation. So a lot of times you're very much inclined to play this game really well. And it's fun. It gamifies it. Another game that I played with our women in cyber Security group is a it's an acronym bingo, cyber bingo. So we'll play bingo based on all the acronyms and explain them. So then you're kind of gamifying the experience, and you're learning while you're having fun. So instead of kind of the meetings where we all kind of show up and we're like ugh, another meeting, you know, to take some notes, got to talk about this. It makes it more fun so you can walk away with an experience and you learn something new, right? So, you know, we're trying to do things a little bit differently and work with our partners, our brokers, our insureds to make sure that they walk away learning something and not just being talked to, we're not just trying to talk to people were trying to actually educate them.

[Kevin]: So two points I thought of when you were saying that. First is it's not just the game, it's your gamifying it, but as an organization you have... you are responsible for your incident response and for complying with the applicable law. So you're going to make a game of it. But the game is critical because you're developing that, I like to say "muscle memory," so that when there is an incident, you've done it before and at least some

form. And the other thing I was thinking is in you, you exemplify it, Brandy, is that your insurance carriers... Crum & Forster is is a terrific example—have resources that a business can avail itself of you know, you can use your insurance company to help review your incident response plan. They may have resources for you, tabletop exercises or running that plan so that you're more comfortable. And whatever you learn from that plan, your carrier may or may not have some advice for you that you can consider in upgrading your system. So the insurance industry really has played, I think, the leading role in cyber response for the last 10 years. It's much to the industry's credit, but because of that, there are so many resources out there and if you're not taking advantage of them, you should talk to your carrier and your broker and find out what's there and take advantage of some of them, because you may be surprised and it may make it a lot easier to respond to a cyber incident when that inevitable thing happens to you.

[Brandy]: Right? Yeah. And you know, some other services, there's so many, you know, and you hit a good note there. We have a web site, right, that our insurers can access and they can do external vulnerability scans. They can run phishing assessments and training assessments. There's a policy template library, right? So they can either look, see if they're doing great or maybe if they need to improve and grab one of those templates for their organization. So there are a lot of free resources that otherwise you'd have to pay for. So I think a lot of people need to know what those resources are and take full advantage of them. There are a lot of state resources for specific industries, a lot of federal resources, CISA, for specific industries. I've talked with a lot of insureds recently who are using those resources to do web application scanning, to come in and have conversations with the local FBI agency to kind of talk about preparedness. We had another claim where the FBI actually reached out proactively to an organization to say, hey, there are some indicators here that you're being attacked. You may not be aware of this. They were. And, you know, and so we see a lot of proactiveness as a whole from our local, state, and federal governments that are really helping. So if you can maximize the benefits of your carrier, of those services, and you can save a lot of money overall and you can have all the resources available to you for the most part while you're trying to build/mature your cyber security program.

[Kevin]: Yeah.

[Brandy]: And then the other thing I'm sorry.

[Kevin]: No, go ahead.

[Brandy]: For me personally, you know, I again, I'm new to the insurance industry, right? I'm much more embedded in the cybersecurity community than I am in the insurance community. And that will change over time, of course, as I get settled in. But where a lot of folks go to all the insurance conferences, plus, net D and so on, I go to a lot of the local Atlanta cyber security conferences and I do hear, you know, people talking about insurance right. Saying the applications are like an audit and, you know, insurance doesn't pay. And it's great for me to kind of be in that room and have the conversation as a cybersecurity professional. And now someone who works in insurance to say that, you know, hey, answer the applications as accurately as possible, make sure the right people are answering the applications, provide context, have conversations, and, you know, honestly follow the process. And insurance is a really great way to make sure that you have that coverage in place when something happens. You just have to understand that this is also a business; we want to be around to continue to offer insurance coverage for the years to come. So we need to manage risk appropriately. We need to understand what your risk is. And we can only do that by getting the right context of what's going on within your organization.

[Kevin]: Well, Brandy, that is a great point, and I think that's a great place to leave it. Thank you so much. We begin with risk assessment and with that concept, too. So very important in the insurance industry and in this process of making sure that you have the right kind of insurance in place for your business.

[Brandy]: Yes, absolutely.

[Kevin]: Well, Brandy, thank you so much for coming on Cyber Sip. I really appreciate it. I hope you'll come back soon for another episode.

[Brandy]: It's always great seeing you and worked with you before in the past, so that's always awesome. So thank you so much for having me. Enjoyed the podcast and hope to see you again soon.

[Kevin]: Yeah, same here. I appreciate it. Brandy, thanks so much and thanks to 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.

Disclaimers:

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.