Barclay Damon Live Presents: The Cyber Sip Podcast™
Episode 24: "Avoid Cyberattacks: Don't Click That," With Rich Sheridan

Speakers: **Kevin Szczepanski**, Barclay Damon, and **Rich Sheridan**, Berkley Cyber Risk Solutions

[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]: So we're here with Rich Sheridan, who is senior vice president and chief claims officer for Berkley Cyber Risk Solutions. Rich has been in the cyber and professional lines space for over 20 years and, Rich, it always makes sense to me how an expert in professional lines would migrate into cyber. But as you look back, do you understand that evolution in your own career? Did it make sense to you at the time that you would take on such a significant role in overseeing cyber claims?

[Rich]: It made some sense for sure, because it was in relation to some of the products that I was handling claims for previously. But, you know, when I go back and look at it in my career, you know, I didn't know…it at the first time when I saw cyber as a, you know, a policy as an insurance policy, cyber policies, I didn't imagine that when I saw that that my career would be totally cyber, you know, going down the road about 15 years later. And here it is. This arm of insurance has really grown substantially and dramatically, you know, in the last several years. But I do see it as a natural growth, because there was kind of the technology aspect, the technology, you know, type of stuff I was doing kind of had some relation to that. And those are the underwriters that for the most part got involved in cyber.

[Kevin]: Yeah, that makes sense…that's a podcast episode in itself. How did we all get into the cyber? First question I wanted to ask you and I really want to put us in the mindset of a customer or a potential insured. What…how are you finding the average Berkley customer today experiences a data breach or cyber incident. You know, what are the common types of claims that you're seeing today?

[Rich]: Sure. That's a great question, Kevin. And you know, one thing I think that's been consistent throughout, you know, at least the last 10 years within cyber is, you know, one of the things we just see are just the email compromises where the threat actor gets into the insured's network and, you know, kind of looks to make mischief. They may try to steal data, they may try to, you know, take over the email account and send out fraudulent invoices and get payments on that. They may, you know, try to send out emails from that account to get data from other customers, get them to click on links and fill out stuff, or maybe plant malware in there as well. So we see that, you know, and that's been steady throughout and that's been I think kind of a core cause of loss that I've seen, you know, over the last 10 years that's continued. Of course, ransomware, you know, is something that, you know, going back in the last several years are really picked up in in frequency. And, you know, and in severity. But, you know, it had been out there for a while, but it definitely picked up much more so in more recent times. We also see a lot of…and I kind of touched on with the email compromise, fraudulent payments, you know, that sort of thing where somebody gets in the network and tries to send out, you know, fraudulent invoices or communications, changing bank accounts and trick people to making payments to fraudsters. Those are probably, you know, three of the core type of things we see. And then there's, you know, there's miscellaneous just privacy violations where insureds accidentally send

out emails with personal information on it or, you know, can even be paper copies; they could throw out, you know, like documents containing personal information and leave it unprotected and, you know, leave it in, you know, in a conference room somewhere and expose that data, so...

[Kevin]: I remember getting scolded, and rightly so, years ago by a mentor of mine at my old firm, because we were, you know, I had started giving presentations. The best way to learn a subject is to present on it, ironically enough. And I was talking about hackers and you were talking about hackers as well. But about 10 years ago at a NetDiligence conference, when you were asked this same question back then, your answer was, well, yes, we're seeing hackers, but we're also seeing the old "somebody leaves laptop in the back seat," or leaves a laptop on an airplane. I take it the frequency of the accidental employee mistake–type claims that...at least the ratio has changed. It's not so much employee mistakes that are leading to the most common claims or is it...?

[Rich]: Well it's not employee mistakes to the extent of losing devices or misplacing devices that...it's oftentimes it's employee mistakes and clicking on emails, you know, clicking on links and emails and that sort of thing. Still, you're only as strong as the, you know, as the employees that that are guarding your data. But I think one of the things with the lost devices that has somewhat changed over time. And part of the reason I don't think we see very many of these type of claims anymore, we still see them on occasion, but not with the frequency that we did, is that I think oftentimes with, like lost laptops today, most laptops will, you know, in the work environment will be encrypted and I think when people lose laptops, a lot of times they just don't get reported because there's no concern over data being lost since they're encrypted. And the same probably with you know, with other personal devices like phones as well, you know, so and you know, also multi-factor authentication, if the device is equipped with that, I think there's less concern. So, I do think to some degree, maybe employees have gotten a little more careful with it. But I also think that the degree of these matters being reported is not as high because of the encryption of the devices and the lack of concern that data can be exposed.

[Kevin]: So that's a good point. Encryption has changed the landscape there. Let's talk about litigation trends. And again, back 10 years ago when you were you were at the NetDiligence conference. And if anybody's interested, check this out on YouTube, it is the Pythias 10 minutes you will see, and Rich is asked about 20 questions and they cut it into 10 minutes. One of the questions was about litigation trends. And back then the answer that you gave was something like, well, we are seeing litigation, but it's mostly arising out of the big data breaches against...involving big companies. Has that changed in the last 10 years? So if I'm a customer coming to Berkley and I'm saying, you know, Rich, what is my litigation risk? How do you answer that?

[Rich]: Yep. And I think it has changed. And a couple of things have changed in the climate. First, there are a lot more state statutes and international statutes, frankly, that, you know, deal with the protection of personal data and privacy violations arising from it. So we do see more, I think, just even on large data breaches, we see more litigation, you know, as a result of those statutes, things like the California Consumer Protection Act, CCPA, is certainly, you know, causing a lot more litigation to be filed both on a larger and smaller scale. And we'll kind of get to that smaller scale a little bit. But, another thing that's I think is encouraging more litigation is some of the larger litigation that's happened. You go back 10 years ago, the amounts of the settlements were you know, they were significant, but not to the same scale that they're significant today. If you look at, you know, the present day, in the last year, we've seen, you know, several you know, I can think off the top of my head within the last year of one large scale, the litigation itself for $190 million another that settled for $350 million and another that settled for $60 million. Now, there were no settlements approaching that scale of going back ten years ago. So that certainly has the plaintiff's lawyers kind of eager to explore this litigation. But I think the one of the big changes is, too, we are seeing smaller scale litigation. It's not... if you see a breach with 5,000, 10,000 people impacted, I would say right now, you're more likely than not to see a third-party

claim, you know, and a lawsuit arise from it. Whereas if you went back 10 years ago, I don't think you would have seen that at all because the state statute schemes wouldn't have necessarily, you know, supported some claim, some of those claims. And also the amounts of the settlements that are out there. I don't think we're making it worthwhile for plaintiff's counsel to even explore it. So I think the litigation landscape has changed as a result of that.

[Kevin]: I think it has too. I think the big plaintiff lawyers may be going against the big companies, but the smaller local lawyers are going up against the local companies. We have one right now, a retailer. There was a ransomware incident there. It was handled well. But we've... we're facing a state court class action. It small business. And that would not have happened even five years ago.

[Rich]: I agree with that. Absolutely.

[Kevin]: So I could get sued. What about investigated? I've got a breach. And it involves the let's say I'm a health care provider and I've suffered a data breach. And I had many, many tens of thousands of records. Only about 500 to 1,000 of them were affected. So that's good news to some degree. But I've got to report that to federal and state authorities. What trends are you seeing there? Are the authorities more likely today to call or write and begin inquiries and investigations than they were a couple of years ago?

[Rich]: Yeah, I definitely think so. You know, on the federal... any time there's a health care breach, still at least some degree of federal inquiry into it, you know, depending on the facts and circumstances. And obviously, the, you know, the worse the behavior of the insured or, you know, the worse the incident is, the more likely they will get involved with that. Yeah, but one of the things we also see now is with some regularity, there are some state attorney general's offices that will make some inquiry based on breaches involving fairly limited number of individuals in this one state out there, Indiana, that pretty much any time there's, even if, as I understand it, even a single Indiana resident is impacted by a breach, they'll make an inquiry that requires, you know, response and requires a little bit of legal work to do it to deal with it. So some states are pretty regular with their, you know, their type of enforcement on it. So. Yeah, definitely. That landscape has changed from five years ago. You wouldn't see that with the same frequency that you do today for sure.

[Kevin]: Now, we're seeing it in New York as well, with the Department of Financial Services.

[Rich]: DFS.

[Kevin]: If you report, even if there isn't a breach, if you are required by law to make a report, you will get an email from someone. They want to set up a phone call. They want to ask you. And that's just that's only going to get more intense, I think, as time goes on.

[Rich]: Yep, I agree with that.

[Kevin]: So yeah. So, so I wanted to shift gears and ask you a little bit about security controls and the trends there. So are you seeing in the claims that you're overseeing, some common threads, some security controls, perhaps like MFA, multi-factor authentication or passwords that perhaps weren't in place or weren't as strong as they could be. And that may then have contributed to either the initial breach itself or the ability to manage or respond to the breach.

[Rich]: For claims that I'm seeing it, it seems to be a variety of things. You know, that that MFA certainly has come up on occasion, where insured doesn't have it and that's a means into entry. You know, sometimes they can, you know, leave...There can be mistakes in portals that they have that if left open, you know, that allow, you know, allow threat actors in. But I haven't found there to be like one

single consistent problem. It can be a variety of issues that can happen. It's sometimes, you know, frankly, it's just an employee clicking on a link, you know, that that got through somehow...the email got through and you know, they didn't follow the precautions that they should have in doing that. I still think that the employee ultimately it's you know, it's individual employees that cause more of the problems maybe than any technical aspect of the response. But, you know, one of the things I do see that's encouraging is I see more and more insureds—and I think the insurance industry as a whole has been pushing this, and just as you know, it's become more heightened awareness—I think MFA is becoming more and more common. I think, you know, training of employees to not click on the link is becoming more and more frequent and insureds being more prepared overall, I think that's part of...when they buy cyber insurance, insurers are pushing them to be more cyber aware. And I think we're seeing that a little bit in our industry. And of course, the bad guys keep getting smarter and find other vectors of attack, you know, to come around this. But, you know, it's rather than give them low-hanging fruit, I think insurers are getting a little better about things. Yeah.

[Kevin]: So speaking of insureds, someone comes to you today or better yet, Rich, you have an opportunity to speak to every insured of Berkley Cyber right now. What two or three things would you want to tell them? I remember the old days. Was it "The Flintstones" where Mr. Slate had the microphone on the desk? He could talk to everybody. I imagine that occurs to some degree. I wish I could tell everybody this right now, and it can't happen. But actually, you can right now on Cyber Sip. So if you had that opportunity, there were just one or two things that you could tell everyone that you think would improve response to data breach or other cyber incident. What would it be?

[Rich]: You know, MFA is definitely on the list, and multi-factor authentication...just I assume listeners are aware what that is, but just in case.

[Kevin]: Some are not. Some are not.

[Rich]: Yeah, some may not be. That's true. You know, it's something we live and breathe, but I know not everybody does. Right.

[Kevin]: So and just to be just so our listeners know, so that is not just your login and your password, that is in addition to your password, which is one layer of authentication. It's something you have either a token, something you know, like the answer to a security question or increasingly something you are; biometric information, retinal scans, fingerprints, something that makes so unique that it's very hard, if not impossible, to duplicate. So back to you on MFA, Rich. What are you seeing there? I often see situations where there is MFA capability on a client's system, but it hasn't been enabled. And unfortunately we don't learn that until we're responding to a data breach. So what's your advice there?

[Rich]: Yeah, enable it. And also when you have MFA, have it, you know, 100% of your employees and your endpoints protected by MFA because, if you leave certain areas open that that's a way to get in, you know so we've seen insureds that that have MFA but they don't have it you know 100% across their system. You know, and access is gained through a non-MFA protected device right so it's important to just do it thoroughly, do it thoroughly. So yeah.

[Kevin]: What besides MFA, if you had again you can speak to everyone at once. MFA, I assume smart passwords—which by the way, we should say we, you and I use these terms, but I learn from our our listeners and viewers: Everyone does not always have the time to master the cyber lingo. So we're talking about smart passwords, not necessarily your name or your children's name, certainly not the word "password" or 123456 which are, I believe, still the more common passwords.

[Rich]: Exactly.

[Kevin]: Just incredible. But it's true. Yeah. So by a "smart password," you're talking about combination of large and small caps, letters, numbers and symbols and length, 12 to 14 of those symbols that make it very difficult, if not impossible, for either a threat actor or an algorithm to guess. Yep. So we've got MFA, passwords. What else would you tell everyone, if you could, to do right now that would improve their cyber hygiene?

[Rich]: And one of the things we see and, you know, I touched upon one of these cause loss is fraudulent payments. And, you know, one of the things about the fraudulent payments, it's typically done by some email...fraudulent you know, a communication by email from an imposter pretending to be somebody else, either, you know, a customer/client of the insured or, you know, the CFO, you know, demanding a payment of some sort and giving change information. And I see so many of these and they could be prevented by picking up the phone and calling the person and using...don't use the contact information within that email. Use it from something independent to do it and you know, 98% of these, if not more, would be prevented by doing that and having that process in place and followed would prevent so much of the fraudulent payments that we see out there.

[Kevin]: I think that's yeah...

[Rich]: I was going to say that's one of the things that I see. It's like, I shake my head every time I see it. But it's, you know, it's a relatively simple fix.

[Kevin]: No, we do too. And just so everyone can appreciate this, the threat actor is not going to be able to steal unless the employee directs payment to a different routing number and account number. So if you get an email that says we're changing our account information, please send your payment to the following routing number and account number you...the red flags should go up...

[Rich]: ...and alarm bells Yeah, everything.

[Kevin]: And pick up the phone and call and say, hey, I just got this email from you that says you're changing your account information. Is that correct? And 98% of the time they're going to say, no, it's not. And by the way, just so you know, we would never change our account information by email. We would contact you by phone, or we would send you an encrypted communication. Those are always best practices.

[Rich]: Yep, absolutely. Absolutely.

[Kevin]: Well, Rich, this you've been very generous. Thank you for all your time this morning. I really appreciate it. Thanks for being a guest on Cyber Sip and I hope you'll come back again some time and talk about the next hottest topic.

[Rich]: Yep. My pleasure, Kevin. I appreciate you having me on. And I enjoyed our conversation.

[Kevin]: Thank you so much. And thanks to all of you. 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.

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.