Barclay Damon Live Presents *Cyber Sip*™ Episode 35: "The Future of Cyber Liability Coverage," With Reggie Dejean

Speakers: **Kevin Szczepanski**, Barclay Damon, and **Reggie Dejean**, Lawley 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]: Welcome back to *Cyber Sip*. We are pleased to have back with us Reggie Dejean, director of operations at Lawley Insurance. Reggie, welcome back.

[Reggie]: Thanks, Kevin. Thanks for having me back.

[Kevin]: Oh, no, thank you for joining us. And, you know, in our last episode, we talked about the question, do I really need cyber insurance? And your thoughts were so helpful there. I wanted to ask you to come back to comment on something and maybe talk us through a quote that's come recently in the insurance world. And it dates back to December 26: The Financial Times reported a warning from the CEO of Zurich Insurance who said, and I'm quoting now, "What will become uninsurable is going to be cyber. What if someone takes control of vital parts of our infrastructure? The consequences of that." And then he goes on and in response to a discussion about the privacy risk to individuals, he says, in effect, you know, if we're focusing on the privacy risk to individual, and the risk of lawsuits for those who suffer identity theft and so on and so on, we're really missing the big picture. And he adds, and I'm quoting, "First off, there must be a perception that this is not just data. This is about civilization. These people can severely disrupt our lives," close quote. So The Financial Times interviews the CEO of Zurich Insurance, Mr. Greco. And Mario Greco says, I'm seeing a day in which cyber risks are going to be uninsurable. What do you make of that, Reggie? Is that true? And if not, what do you think he meant by that?

[Reggie]: Well, I think it's kind of like just throwing up a flag and saying that, you know, we need to be careful of what we're doing as we go forward. Zurich is a big writer of cyber liability, and we have worked with them. We've paid claims with them. So we know that what he's saying is real. As far as you these payments being made. What I will say is that some insurance companies buy insurance itself, so they work with what we refer to as "reinsurance" in the insurance world. What we're seeing there is that these reinsurance companies, they don't only insure cyber risk, but they ensure property. And you look at the number of claims that are happening out there just on the property side. I heard something yesterday talked about that said 80 days between $1 billion event. We have now come down to under ten days between every billion dollar event, billion with a B, in the insurance industry. So when you start to aggregate that and you think about where some critical exposures are, cyber liability is certainly at the top of the list. I mean, because that went from zero claims, because there was no policies written maybe 15 years ago to now we're kind of leading the pack as far as the number of claims. So the insurance companies and their insurance companies, the reinsurers have been hit really hard in that area. So when you look at this, I mean, this isn't the first for insurance. You look at the flood program and how that works with the federal insurance. And then you also look at the terrorism act that was passed, the 9/11 attacks. So this is a potential first cry from the insurance industry stating that, hey, we may need a backstop. We want to insure this, but we may need protection from the government, as far as,

you know, similar to the Terrorism Act that was passed. We may need some type of cyber liability legislation in place. So that's I guess that's what I got from it, as opposed to the coverage of stopping cold turkey and not writing coverage anymore.

[Kevin]: [Media] coverage sometimes has a habit of taking a quote, lifting it out of context and plunking it into a headline and it grabs attention, but it may not be exactly what was intended.

[Reggie]: Yeah. So we do see that. And I do believe that that's the case. And I haven't heard too many other insurance companies echo that. I have heard the concern about ....

[Kevin]: And that concern it strikes me as not just about the privacy risks to individuals. As he said, he's not talking about the class actions that we're seeing in the United States, individuals whose names show up in data breach lists are bringing lawsuits alleging violations of privacy. He's talking about something more along the lines of a systemic risk. We hear that term frequently, particularly over the last year, but I don't think many of us really understand what that means. Reggie, can you talk a little bit about what a "systemic risk" is and why it triggers so much more concern on the part of leading insurance companies than these, dare I say, smaller risks involving individuals just bringing privacy claims?

[Reggie]: Yeah, so think about the pipeline that the damage that cause actually some physical damage as well as just not being able to provide gas for a good portion of the northeast. A couple of years ago.

[Kevin]: And that was Colonial Pipeline. Yes.

[Reggie]: Yeah. So when you consider that, I mean, you have these actors that all of a sudden they're taking over, you know, major utilities and that could cause some significant damage to not just the loss of an individual, but the loss of many companies. Again, that's one of the issues that the insurance companies are grappling with. And one of the things that came out of 9/11 was, you know, whether it was an occurrence, it was the two buildings, unfortunately, that came down was one or two. And how much more that cost the insurance industry by having two losses declared with the two towers coming down. So I think that's what you're really concerned that you're seeing in the insurance industry, particularly in this case. Now, let's look at what happened just yesterday with the airline. I mean, there's no indication that it was a terrorist or cyber-attack. But when you see something like that, the infrastructure where for 90 minutes we were grounding all flights. Now, what if that was a cyber situation? So it's much greater, just than one or two losses. It's really across multiple of parts of the industry.

[Kevin]: And these are risks—when you talk about the pipeline industry, you're talking about energy, you talk about airlines, you're talking about national and in global transportation, these are the sort of large systemic risks then that can transcend individual policies and companies. And like we see with hurricanes, cost the industry and everyday folks billions and billions of dollars.

[Reggie]: Yeah, we're definitely seeing that that is a significant concern.

[Kevin]: So one of the responses to this threat of systemic risk that I've seen, Reggie, and I want to ask you about it, is the offering of exclusions to cyber insurance policies. There are some exclusions for what's called "war-like action." There are other exclusions for what is called a "state-based attack." The... it strikes me, though, that one of the problems with that is that if I'm buying a cyber policy, I have insurance and I know there's this exclusion in my policy for war-like action, but I'm not going to know until... if I'm attacked after the attack, I may learn that it was instituted by a foreign state. We know who those states are, but it's difficult for me to plan and understand whether I have insurance in place if I don't know until after I've suffered the loss, whether the exclusion applies. What are you seeing when it comes to these war-like exclusions or state-based action exclusions? Are you seeing them in the policies that carriers are offering now? Tell us about your experience in that regard.

[Reggie]: Yeah, so we are starting to see more exclusions coming on policy. We're seeing co-insurance, which is basically where you share in the loss. If it's $100,000 losses, 50% co-insurance, you pay $50,000, insurance company pays $50,000. So we are starting to see some innovative ways that the companies are trying to minimize the loss side of things. But these exclusions are real and there are some companies that are pushing them more aggressively than others. You know, as a broker, what we try to do is push back against the insurance company, and if they don't want to, you know, concede that they're going to take those exclusions off, we will look at other options because as of right now, there are other options, maybe a little more costly, but certainly might be beneficial for a client. So those are some of the things that you can take a look at when you have those exclusions in there. The other thing that's probably a bigger issue for insurance companies is that these are kind of untested endorsements and exclusions.

[Kevin]: Right?

[Reggie]: We've seen where the courts are not too... they tend to side with the clients and they do with insurance companies when they try to invoke these exclusions, because generally what they come back and say that it's not for the insurance company to decide whether it was an act of terrorism or war. That's for government to declare that. And we just don't think that is going to hold up. But we are seeing these endorsements as least right now, they're being tested.

[Kevin]: That's a great point. I mean, in the courts, exclusions are interpreted narrowly. So that favors the policyholder. Also, I think it's a problem because it's just very difficult sometimes to identify the source of an attack. It's one thing if North Korea comes up the next day and takes responsibility for an attack. But most states, in fact, I'm not sure any state has a practice of coming out and saying, yes, we were responsible for that attack on the United States or on this industry sector. So I think it's going to be difficult for... I think it's going to lead to litigation. But I think ultimately it could prove difficult to enforce those exclusions unless you have some sufficient proof that a state actor was involved.

[Reggie]: I agree with you completely. We can put the situation where, you know, an innocent party can have something that their computer systems maybe used to override somebody else. And so now you can say that to come from so you can have the use of bots, you can have millions of different computers that are attacking your company. So how do you actually determine who ultimately is going to be responsible for that and actually determine that it's actually an act of terrorism or an act of war or something along those lines?

[Kevin]: And in a strange sort of way, I suppose these exclusions are meant to maintain the existence of cyber insurance. I suppose on one hand, there are policyholders out there who are going to say, no, it's meant to eliminate coverage and we don't like that. But on the other hand, the industry might say, as Zurich's CEO said, no, no, you misunderstand. The existence of these exclusions for state-based attacks or for war-like acts are actually going to have the effect of preserving coverage. Because if we can narrow the scope of coverage just a little bit, you will have coverage for all other events, just not war-like or state-based action, we will be able to collect a reasonable premium and extend coverage. But otherwise, as Mr. Greco of Zurich says, cyber insurance may narrow if it doesn't go out of existence entirely.

[Reggie]: Yeah, and you want to try to protect that certainly as much as possible. But you know, it is something that I think we're going to see. Again, this is the first in a series of tests. I'm sure we'll see what this exclusions, but it's going to be very difficult to enforce. And I think that there's going to be a lot of pushback. But you're right, we are starting to see where more questions are being asked of companies on applications, including third-party vendors to national vendors and what countries are they in. Sometimes, frankly, you don't even know because you may be using a third party that you've contracted with in the US, but they contract out to somebody who has your files in Ukraine. And so maybe they weren't able to get that information out. So you just never know where things are going to be exposed. But that's why should we have a solid of a policy in place? Insurance-wise certainly. But this your incident response plan and your cybersecurity risk within your

business, you want to make sure that you are asking those questions of you that you know, hey, who will have access to my data? Where is it going to be stored? The more educated you are about it, the better I'll be.

[Kevin]: Right.

[Reggie]: And again, I say this a lot, but the best insurance policy is one that's never used. You know, if you can safeguard your data and safeguard your business as best you can, it's great to have that backstop. But you really want to try to avoid as much as possible being the victim of a cyber breach.

[Kevin]: And that means having the right written policies and procedures in place and having the right security controls in place.

[Reggie]: Absolutely.

[Kevin]: You said it better than I ever could. So I was going to ask you a question about that, but I don't think we need a question. I think you've covered it. I think cyber insurance is here to stay. But I also think it's going to remain tight for a while. And the best you can do as a policyholder, as a small, medium sized business is to make sure that you have those safeguards in place so that you don't need the insurance. That's great advice, Reggie. Thank you.

[Reggie]: Thank you, Kevin.

[Kevin]: Well, I want to thank you so much for coming back and doing another episode of Cyber Sip with us. I really appreciate it. And we've got a webinar coming up later this year. I'm looking forward to that too.

[Reggie]: As am I. My thanks again for having me. Looking forward to seeing you soon.

[Kevin]: And congrats on your new role and your 20 plus years of experience in the insurance industry. Very impressive.

[Reggie]: Thank you, Kevin. Really appreciate it.

[Kevin]: Thank you. And thanks to all of you for joining us for 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.

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.