Barclay Damon Live Presents *Cyber Sip™*
Episode 31: "Do I Need Cyber Insurance?," 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. Today we are pleased to have Reggie Dejean join us from Lawley Insurance. Reggie is the director of operations, which is a new role for him. But for the last 20 years, Reggie has been involved in the insurance industry, including the underwriting and marketing of cyber security products. Reggie, welcome to Cyber Sip.

[Reggie]: Kevin, thanks for having me.

[Kevin]: So today's episode is "Do I Really Need Cyber Insurance?" And I thought we'd start off 2023 with an episode like this because there's been a lot of talk out there about where the cyber market is going and is the market even going to exist in five years. And so I thought we'd return to basics with "do we really need it?" And so my first question for you is when a customer asks you "what is cyber insurance and do I need it," what do you say?

[Reggie]: Usually what I…Thanks for the question, Kevin, but what I usually like to do is start out with the example of a typical claim that we see, because that tends to really answer many of the questions that the client has. But what we see in a typical claim is that it's either usually through email that somebody will infiltrate the system and a user, the employee will click on email and then that will start the ransomware and open up the malware, which leads to the ransom demand and the ransomware. That's when the client realizes that something has happened and they can try to unplug their computer as quickly as they can, but that's usually too late.

[Kevin]: Right.

[Reggie]: The scenario would be that you have a ransom demand that's being asked now. So what do you do there? If you have a cyber liability policy, you have coverage for the extortion or ransom demand. You also have the legal costs, which you're going to almost immediately incur and then also the forensic. And those costs are within the first 24 hours. You know what your costs are going to be because they're going to ask you what the what the ransom is going to be. They're going to let you know what the… what you have to pay in order to free up your data. And then again, the legal and the forensic, the forensic can start almost immediately. Even from a distance, it's amazing what some of these forensic firms can do. So you definitely want to engage them. The part that people don't always think about with cyber liability coverage is the business interruption, because they think about their data, they think credit card information is not that important, that no one's going to really ask me for anything. And to some degree, that may be true, but the business interruption is real. And what happens is that if you have maybe 20 or 30 computers, if you're a smaller company, many times you have to bring each one of those devices back up individually. So that forensic firm is going to be doing that. But in the meantime, we have seen many of our losses that the business may be out between one and three weeks, that they are not able to operate. So the loss of income and all the payroll and everything else that you have to pay for, that business interruption coverage is can be a critical aspect to really saving your business because the statistic is still there: 60% of small businesses will fail within six months of a cyber breach. So that's what we usually talk to the clients about. So if we have those four things the cyber extortion, the legal, forensic, and the business disruption. Think about that first. Even though there are many other coverages involved with the cyber policy.

[Kevin]: So that makes great sense. And now where, you've convinced me, and I want to look into the purchase of cyber insurance. But my next question is, okay, how do I get it? Is there an application process and what information do I need to put together to prepare for that application? Talk us through that and maybe first, Reggie, tell us about how the application process has evolved over time. I know it wasn't too long ago where there were two or three questions on the application and there were no questions about system controls and malware and so on. So what was it like a few years ago and how has that changed over time?

[Reggie]: Sure. So if you go back about 15 years ago, really, it wasn't so much cyber policy coverage as it was a network security for IT firms, people who were in the network area. And those applications were very lengthy. And over time, people developed, and ACE Insurance is one of the first companies that come up with, the privacy liability coverage form. And that was, you know, maybe six or seven pages long. And then it really… as more companies came in because there are not a lot of new insurance products. So, this was a new insurance product the companies could come in and take advantage of. So they limited the questions to many times, like you're saying, it could be two to three, sometimes no questions other than the obvious ones of the firm name, address, revenue, and maybe number of employees. And then they would put it into a little model and they'd come out with a… with a premium. And many times it was pretty aggressive premium. So you have, where there was no underwriting involved, there was no… very little claims involved. So the market became softer and softer. The questions became, again, non-existent. And then fast forward to right before… COVID. At the end of 2019, we started seeing the losses started to escalate and escalate very quickly. The common denominator was multi-factor authentication, that if you didn't have that, that's how people were really taking advantage of getting into your systems. So then a lot of questions started coming out—to the point now where we're not back up to the 15-page application, but we are, you know, asking a lot of questions on the application, the biggest questions of which are multi-factor authentication. Do you have that in place? And what are your remote protocols, with everybody working remote? What kind of safeguards do you have in place to protect your systems from an intruder?

[Kevin]: So you go through that application process—and thank you for that. So multi-factor authentication, remote protocols, more "kicking the tires" from the standpoint of the carrier. So you complete the application, which is not 15 pages, but somewhere in between. So I've seen five-, seven-, eight-page applications. You complete this application and how does that process work, Reggie? Who's… where are you drawing the information from to complete the application? Who is in charge of the document itself? Really want to give our, our audience a sense of how this process works, because I think a lot of folks don't really understand it and they may not appreciate how many people within their organizations need to contribute.

[Reggie]: Yeah, so the older applications you can pretty much answer by either giving to someone in your IT department or maybe even someone that just deals with insurance on a day-in and day-out basis. Your risk manager—who may not know all the IT issues that are there. It has evolved now where you really need to get… if you have an internal IT department, you want to get them involved. And if you contract out those services, you want to have your service provider take a look at the questions, because they do get pretty technical. Again, multi-factor authentication, or MFA, is a big question. They want to make sure that you have that in place for email…for almost any entry into your system. You want to make sure that those people who have the most access to your system, the administrative codes or privileges, that they have multi-factor authentication in place. And sometimes we get pushback on that. But really, if you think about it, those are the individuals that have the greatest access to your system. So you want to make sure you lock those entry points into your system down. You want to lock them down as much as possible.

[Kevin]: Right. And if you have multi-factor authentication, it can bridge the gap when you talk about the strength of your passwords because you're adding a measure of protection beyond just the passwords itself. And I know the carriers are asking, do you have a password policy? What are your security controls? And also some of the applications ask about employee training. So what are you seeing in that area, Reggie, and what are the carriers interested in when they ask about training programs that the policy holders have in place?

[Reggie]: Yeah, well, you want to have at least an annual training. What we have done here is we are going to a quarterly training. So instead of doing a 45 minute to an hour annual training, we're trying to break it up into 15-minute increments throughout and on a quarterly basis, because the more your employees are aware of what some of the catches are, that they can fall subject to or where some of the, you know, we talk about phishing and you don't want to get the, you know, if that hook comes in, you want to be able to identify that hook before you snatch onto it. So the training for your employees, again, your greatest asset, your employees can also be your greatest point of vulnerability. And curiosity always gets the better of people, myself included. A lot of you find.

[Kevin]: Me too.

[Reggie]: Those you see those emails and you think, huh? I'm not sure if I was waiting for that one, but let me see what it is. Then you open it up and then by that time it is too late.

[Kevin]: Right. If you have not been fooled by one of those spear phishing attacks, you're not human. Especially around holiday time. That was one that fooled me because I had so many packages coming in and I got… I think it was an SMS message from Amazon or maybe it was DHL asking me to confirm some information for a shipment and I did it so quickly because I needed the gifts so quickly that I didn't bother to think that, gee, I don't actually have something coming from DHL or this service provider, and it ended up clicking on a link. Fortunately, it was a test link that was sent to me by my employer. So nothing bad happened. But it's very easy to fall prey to those, isn't it?

[Reggie]: It really is. I mean, we had that in our office. The one that was the most successful was an email that came in with a click to a video or to a picture of a dog in a neighborhood that has been lost. And they're asking people to click on that picture to see if you've seen the dog in the last hour or so. And we got a lot of people with that one, you know, could care less if you're trying to save a human being. But if it's a dog, it seemed to be something that people wanted to click on.

[Kevin]: Creating a sense of urgency. That's what they do. All right. So you've completed your… you've completed an application on behalf of your policyholder and you submit it to a number of carriers, right? And let's say you've submitted the application to five or six cyber insurance carriers, but in response, you get a "no" from every single one. Every single carrier has said, I'm sorry, we're going to pass on this risk because we don't think that you're insurable at this point. Have you had that happen to a customer at Lawley, Reggie? And what do you do when something like that happens?

[Reggie]: Yeah. Fortunately, it's very rare that that happens. We had one where it was a client that had been trying to find their… they lost a renewal because they had a pretty significant loss and they were trying to find some coverage. So we went out to the market and the market—because of the type of loss it was—a, you know, it was… they didn't have the proper safeguards in place from MFA or multi-factor authentication. They just didn't any box that you should be able to check yes, it seemed like they had a no checked off on that box and with a pretty sizable loss. The fact that they had some pretty valuable data, it was in that situation that was probably one of the few accounts I can remember that we just couldn't get any coverage for. And, you know, they also… sometimes our clients have contract requirements. So in this case, it was very challenging for us because we knew the client had to provide proof that they had cyber liability coverage, but we were just not able to get it for them.

[Kevin]: Right.

[Reggie]: They did have one option that was significantly less than what they had, so they needed $5 million the limits. They got $1 million, and I think it was like $100,000 deductible that their former agent had as the only option for them. So I guess it wasn't completely "no" to the type of insurance, but it just it didn't fit what they really needed to provide for their clients.

[Kevin]: So let's say a customer comes to Lawley tomorrow, Reggie, and says, you know, I don't know what to do. My prior broker applied for insurance. We were unable to get it, so we're coming to you. What's your best advice to an organization that may have tried to get insurance but was declined that particular time around?

[Reggie]: Yeah. So they definitely... they want to get together and not just you know, there's IT and then there's security companies. So sometimes your IT provider's not necessarily a company you want to go to from a security aspect, right? So there are some that they do both, but you want to make sure that you're working with somebody that's really strong on the security side of things and had them take a look your system, make sure that you do. In this case, you may have to provide a summary of a penetration test or any type of testing that the security company is going to do once they implement some of the procedures that you really are going to need to implement. IT security is no longer optional. It is a cost of doing business. So we certainly would tell the company if they weren't prepared for that, that they have to budget that into... that they had to make sure that is part of their budget, the cybersecurity piece. And we can try to refer them to either a law firm or forensic firm that the IT security company is going to be able to help them out because really from a legal standpoint, you want to make sure that they're working with a law firm that's going to be what sometimes is referred to as their breach coach. That's going to be the first line of defense when something happens. So if you get that next potential claim, you're going to call your law firm that you're working with. And then usually they will be the one to contact and get a hold of forensic firm, as you know, because that keeps everything privileged and confidential as much as possible. When you do have the legal firm involved right from the beginning.

[Kevin]: So, Reggie, even if an organization is unable to get insurance, you're saying that they should still take that step to vet a law firm who can serve as a breach coach, a forensic vendor who can respond to the breach, and maybe even a ransomware firm who can be called on if there's a ransomware attack. The company should have those pieces in place, even if it doesn't have insurance, so that it knows who to turn to when that inevitable cyber incident happens.

[Reggie]: Correct. Yeah, It's equated to your furnace goes out, you know, December 24 and you have guests coming over or you have guests in the house, plus more coming over on the 25. You know, you want to make sure that you have a contractor in mind, you're going to pay more, but you want to make sure that you have something that you can get a hold of. And the same thing with the legal and forensic. You want to have those contacts in place, never mind the fact that you ought to have the fee structure in place. God forbid something happens, because I can pretty much assure you that you're not going to have a claim that's going to happen between nine and five Monday through Friday—that it's going to be on a weekend when you least expect it and you're most vulnerable, because guess what? That's when they can get the ransom demand out. Yeah, quickly, because you are in that situation.

[Kevin]: Yeah. You want your breach coach, lawyer on speed dial and you don't want to be meeting that lawyer or the forensic firm or the ransomware firm for the first time. When you suffer the breach, you want to have met them and vetted them in advance. That's great advice. Thank you so much. I know we're out of time. We'll leave it there. But thank you so much for coming on and I'd love to have you on, on another episode to talk about a comment made about the existence of cyber insurance came recently in December last year. And I'd love to have you on to talk about it sometime.

[Reggie]: Kevin, thank you again. I appreciate being on and I look forward to seeing you soon.

[Kevin]: Thank you. So much appreciated. Reggie Dejean of Lawley Insurance, thanks to all of you for joining us. 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.