Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 16: "The Power of Cyber Insurance, With Laura Zaroski"

Speakers: Kevin Szczepanski, Barclay Damon and Laura Zaroski, Managing Director - Law Firms Group, Arthur J. Gallagher & Co.

[Kevin Szczepanski]: Hey, everyone, this is a Barclay Damon Live broadcast of Cyber Sip, practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

[Kevin]: Welcome back to Cyber Sip. We are back with Laura Zaroski, managing director for Gallagher's Law Practice. Welcome back, Laura.

[Laura Zaroski]: Thanks, Kevin.

[Kevin]: We did not have time to talk about. No, thank you. We did not have time to talk about everything we wanted to discuss in our first episode. So we wanted to bring you back and continue our discussion. And I don't know if the folks who have seen our first discussion with you, if not, you can check it out on Barclay Damon Live or Spotify or any of the other places we are. But we left off with the submission of law firms' insurance application to the marketplace of carriers. I want to pick it up there. So when you're sending out this application, Laura, what specific types or categories of coverage should a law firm be seeking to place?

[Laura]: Well, definitely we've just seen a change in the coverage offerings over the last year, just due to the proliferation of all these cyber claims. So a lot of carriers are now supplementing coverage and pulling back on coverage. That was pretty commonplace in the market before. So I would say as a law firm, what you definitely want to find is the ransomware coverage. This is going to cover you for those extortion demands. And that's one of the number one things we're seeing law firms get hit with. A lot of our carriers are now starting to supplement that coverage. So I would say definitely you want your broker to find you full limits on that ransomware coverage because it's a key coverage for law firms. Second, in tandem with that, too, is the business interruption insurance, because while you're locked up, you're losing money, you're not billing, you're not working, you're not accessing your system. You may be able to do some tasks, but that business interruption coverage is going to cover that downtime, that lost income, which can be extremely significant sometimes as much as the extortion demand.

[Kevin]: Right.

[Laura]: And again, you've got costs. You know, don't just look at what a demand might be against the firm. You've got to pay your extortion demand. You've got to get forensics and to figure out if they've locked up your system, how to unlock it, how to recreate, how to fix it. And then you've got the component of the business interruption for that time down. So a lot of things go into your policy and you need to examine that exposure to see what type of limits your firm should be buying and the volume of data that you have

and that you store. So that's kind of a calculation, and that takes some time to do, so make sure you do that calculation and spend that time so you're making sure that you have the correct limits on your cyber policy.

[Kevin]: Now, Laura, you mentioned ransomware, but of course, there's a significant issue these days with not only the Biden administration, but really the Biden administration has just continued the trend of strongly discouraging both individual organizations and insurance companies from paying ransoms, not only because it raises a moral hazard, the more ransoms you pay, the more ransomware there will be. But also because a lot of the bad actors are on the OFAC sanctions list. And if you inadvertently pay a ransom to someone who is on the sanctions list, you yourself as an organization could be subject to civil or criminal penalties. So with all that said, I can hear someone saying, why then should I bother to purchase ransomware insurance if I might not have coverage for the ransom payment itself? I take it it's still a good idea. Talk us through why you should still have that coverage, even if you end up not having coverage for the ransom payment itself.

[Laura]: Well, that's where the carriers really come in handy because this isn't something you're figuring out on your own. And attribution has always been a really tough issue because everyone tries to cloak where it's coming from. I know the carriers right now are not paying anything with the Conti group, but they've pretty much shut down a bit, I think and pop up in other places with new names. But attribution still is really tough. There is that OFAC list of what you can't pay, but I know that the vast majority of the extortion demands we're seeing are still getting covered by the carriers. So it's not like there is you know, that's an illusory coverage that's thrown in there. And they're going to say, oh, no, sorry, wrong group. So unless they can truly attribute it to somebody that's on the no-no list, those payments are still being made. And there's plenty of other actors out there, bad actors in places that that we still pay. So it's absolutely a worthwhile coverage. Still, again, if, unfortunately, you would be one of those groups that you can't pay, there's so many other components that still get funded. And we mentioned that last session, the forensics, the business interruption, all the other things that are going on in the background and that still would absolutely be covered by your cyber policy.

[Kevin]: Yeah. So it's critical and helpful coverage even if you end up not having coverage for the ransom or if you end up deciding not to pay the ransom. I think that's a common misconception. Just because you are predisposed against paying a ransom doesn't mean that ransomware coverage is not an important risk management tool.

[Laura]: And there's so much more that comes with the coverage. I always like to point out the free risk management free...

[Kevin]: Yes, yes.

[Laura]: services. Yeah. And even if you never use the policy, those can sometimes pay for the policy itself. And this can do, you know, include free cyber risk assessments. Kind of take a quick look over your system and see what you have, what you might need, things you might need to upgrade. There are sample breach response plans. If you don't have one in place, heck, don't draft one. Take a look at some of the samples and then make one that fits your business. There's a whole bunch of vendor resources and partners that your carriers have already partnered with to help you with legal, PR, or any of those things and even pre-breach at much better rates than you would get on your own. So, you know, I know on our... Gallagher's site they've got free training on there as well for social engineering scams, phishing scams, you know, just extortion scams, all that type of, you know, ten-minute little vignettes you can launch and show to your workforce that really help educate and keep you up to speed on the latest. Articles. Recent breaches, all that kind of stuff is free and usually comes with, you know, working with certain brokers as well as working with certain carriers. So that's really a help to our insurers and something that they surely access because it's free. As we

mentioned, it is free.

[Kevin]: Right? You did.

[Laura]: Right. And that's...we do like free...

[Kevin]: We do like free. And I think so often that is forgotten. We hear everyone talk about how difficult it is to compare cyber products side by side. They're not standardized forms. It's very difficult to compare apples to oranges. But one of the things that's ignored is precisely what you say, which is perhaps the industry makes up for that difference in manuscript forms by offering all of these extra tools to really catch up your organization in cyber hygiene. No. So that's helpful. Thanks for mentioning that. Now on that note, one of the questions that I often hear and I'm sure you hear it, too, is, you know, well, that's all very interesting, Laura, and I appreciate the extra tools, but I don't really need this product because I already have LPL. I already have lawyers professional liability insurance, I already have crime coverage. What am I getting in a standalone cyber policy that I don't already have with all of these other insurance products that I pay for year after year?

[Laura]: Yeah, that's a great question, Kevin. And I get that routinely. You know, this is covered under my LPL, isn't it? I don't need this, this new cyber. Well, you know, definitely, since cyber has come on the scene, different types of coverage, everyone's tried to say, no, this is what this line's supposed to cover. This is what cyber is covering. And definitely that's been crafting over the last ten years to make sure everything falls neatly within different policies. The big thing between your lawyers professional and the cyber is what we call first-party coverage.

[Kevin]: Right.

[Laura]: So your LPL is for when one of your clients sues you for what they consider to be bad services and that you have to wait till someone sues you and creates an action against you. And that's when the coverage is triggered. Cyber is not that way. It comes in right when there's a first-party loss. And that means a loss just to the law firm, and it doesn't require any client to be involved. So like an extortion demand, an intrusion on your system, or releasing a bug in your system, all those type of things that you need to remediate and fix that all those costs that are coming out of your pocket without any other party being involved. Those first-party costs are all covered under the cyber policy. Again, if you have an intrusion, you need forensics to come in. Get you back up and running, remediate, make sure nothing else is sitting hidden somewhere in the corner. All those things were, again, first-party costs. So you definitely need a cyber policy to address those. And many times your cyber is going to be doing all this first-party stuff, before you may even get sued by a client and that's what would then trigger your LPL and possibly the cyber. But you might have blown through your whole cyber limits before you're even at the point where a client sues. So, that's a big difference between the lawyers malpractice and the cyber policy.

[Kevin]: Right. I think that's a critical point, just to underscore it. Whatever insurance you have in place, your liability coverage is not going to pay for your breach coach, what law firm is not going to pay for, you're... the forensic firm that's going to figure out whether the bad guys got in, where they went, what they looked at, what they took. And it's not going to pay for your administrative and breach response costs. So that's critical, Laura and thanks for that.

[Laura]: Then the LPL, too, Kevin, are putting exclusions and for those type of things as well where it wasn't maybe clear a few years ago, many are making that quite clear. And also I always note, I mean you want the cyber claims folks dealing with the cyber breach. You don't want your lawyers' malpractice trying to respond to a cyber breach.

[Kevin]: Right.

[Laura]: Neither are equipped to do the other side of the fence. But definitely when they both are working together, if there is some overlap, then you have both of their expertise to come up with the best result for you.

[Kevin]: So no, that's a great point too, because it is such a highly specialized claim and response. Let me ask you this, on that note, Laura, I'm sure you see this. What's your take, and I imagine the clients will come to you and say something like, well, I have a D&O or, you know, policy in place with an endorsement that adds cyber coverage to it. So I already have this rider in effect. So I'm covered, right. Can you talk to us a little bit about how you approach the difference between maybe, to the point you were making earlier, a different type of carrier offering extra coverage in the way of cyber liability versus a standalone cyber insurance policy from a cyber carrier.

[Laura]: Right. Well, those are little endorsements that were we were seeing added on to policies and we've seen them added on to all sorts of GL, property, any type of policy. Those were kind of the early years where nobody was buying cyber or understood cyber, and the risks were much less. Most of them were add-ons are free or a few hundred dollars, can very shaved down cyber. Very limited coverage many times $20–25,000 in coverage of that type. Right. So that ...we've way surpassed that and the risks of way surpassed that. The evolution is now on to a standalone policy. Many carriers will not do those riders or add-ons most of the time. Most of the time, if you did have a breach, they were just tendering that $25,000 you and saying you're on your own to figure out what to do. One of the great things about the cyber coverage is that you have a 1-800 number or an email or somewhere to get a hold of immediately. If your system is locked up, your entire law firm is shut down, you need to get a hold of somebody and you want somebody on the phone in 10 minutes to start helping you recover. And that is really one of the greatest things about this product is its immediate. I used to liken it to kidnap and ransom. You know, you got the bloody finger in the mail, you don't tender it to your carrier and hope to hear back in seven days.

[Kevin]: Right.

[Laura]: This is a 24/7 coverage and 24/7 response, there used to Fridays and weekends and holidays. That's when all these breaches happen. And that's when they're going to be there for you.

[Kevin]: No. And you're right. And in our experience, clients, whether covered or not, want that, they want to be able to sit down and have a phone conversation and know that the wheels are turning, and that the response is ongoing. And if it takes too long, you don't have an experienced carrier or claims response team, that's problematic. And I think another...I wonder your take on this, I think. As the market has evolved, another reason you're seeing fewer and fewer of those so-called endorsements extending coverage is carriers want to be very clear what they are and are not agreeing to pay for. And we're seeing that more often in the traditional forms where a CGL carrier, a D&O carrier wants to make absolutely clear whether or not that policy responds to data protection, privacy, or cybersecurity claims.

[Laura]: Right. And, you know, Lloyd's has been big at addressing that—or they call it the "silent cyber" problem.

[Kevin]: Yes.

[Laura]: Which has been if it isn't excluded on all-risk policy, it must be included. So I think all the policies coming out of London right now have to address whether they are or they are not intending to cover cyber. And that's why I think even domestically, you're seeing carriers start to define what they are

and what they are not covering. Again, so those risks fall—and I was going to say neatly, but I'm not sure if it's ever quite neatly, right—is this going under my lawyers policy? Is this going under my cyber policy? Is there a component in my crime policy? So, again, you don't want gaps, but you'd also like to avoid overlaps. We don't mind overlaps as much as gaps, because sometimes we can stack policies together and sometimes we have had to, to reach the loss amounts. But sometimes people have had just a gap between two policies and neither covered that. And that's really tough for insureds when they thought they had coverage for an incident and they don't.

[Kevin]: No. We should do a separate episode on silent cyber. You've touched on it. Kelly Geary was here a few weeks back and we talked about that briefly and it's helpful when you have a capable lawyer looking for any conceivable gaps or ambiguities in your coverage when you have no other choice. But you don't want to be in that situation, right? You don't want to be arguing that a policy that was never written to provide cyber coverage, whether it's a CGL or more commonly a property insurance policy, actually provides that cyber coverage. What we find is that the carriers are much more interested in pushing back in those situations, Laura, because they feel very strongly that they did not have the necessary underwriting intent to cover those cyber claims.

[Laura]: Definitely. And you really have to fight those, unfortunately, if you're like, a GL policy, because if you do cover it, then you need to cover that for all your insureds. Everyone, even if you get a court and you would win or lose that case, you really need to win it to say, this isn't our cup of tea. We didn't plan on this, where if you're buying a cyber policy, you have a much better argument against the carriers saying this isn't cyber incident, this is a cyber policy. Even as things evolve and things don't neatly fall under some of the cyber policies, I think the intent is there to cover a lot of these situations. And as the insured, as the client, you have a much greater chance of winning that argument or not even having to push that argument because the cyber carriers are stepping up to the plate.

[Kevin]: Right. So much safer and stronger a position to be in. I know we're running short on time. And I want to get to your recommendations. But first, can I ask you quickly, what do you do—we've talked about the benefits of cyber coverage, the application process, the breadth of the coverage, whether it's network security, ransomware, business interruption, breach response, and why it's important to have a standalone policy—but I'm sure to this day, you will still have a client come to you and say, I get it, but I'm not interested. What's the pushback coming from the firm that doesn't want the coverage? And how do you try to persuade that firm that they really do need this extra measure of protection?

[Laura]: Well, if they're not convinced because they do want to safeguard their own information, their own employees information, and the data they get from their clients, if they're not persuaded by, you know, "you could have a disciplinary complaint filed against you based on the model rules." Now, we've definitely seen that outside counsel guidelines, client requirements almost … a large portion of our firms are seeing clients say, I need to see you carrying this insurance or I won't do business with you. Before I release any data to you, you need to have a cyber policy in place. Some of them tell you what limits and someone tell you what coverages have to be in place.

[Kevin]: Right. Right.

[Laura]: If you haven't seen them as a law firm, you're certainly going to see it in the next year or two. You know, certainly the banking industry has already done it. The financial industry has already done it, and insurance carriers are doing it as well. So depending on your client base, if you haven't seen it, a forewarning, you're going to so much better to have it in place and have that not be an issue than racing around at the last minute, trying to get coverage before you can even take a file from a new client.

[Kevin]: Right. I agree with you, Laura. And I see it increasingly as a competitive tool. The law firm that has not only prudent cyber hygiene, but cyber insurance as a risk management tool is going to be more competitive in the marketplace than the law firm that doesn't.

[Laura]: Absolutely. And any certifications, if you can get the ISO certification, that's like gold in the industry, right? So it's great to pursue those certifications and have all that in place and tout how strong you have.

[Kevin]: No. No question about it. Well, Laura, we are near the end of our time, but I want to close by asking you: I'm a customer. I'm a law firm. I'm managing partner, the risk manager. What few things, what recommendations would you have for someone in my position for upgrading their cyber hygiene, purchasing cyber insurance? What should I be thinking about in 2022?

[Laura]: Definitely working with people that do this day in and day out. You really got to know this area that's really specialized and changing so quickly. But the process of going through a cyber application, going through the questions asked by the underwriters, those questions are all being asked because this is where they've seen breaches. This is where they've seen law firms have problems. It's a great risk management tool to go through that process. Our firms are like, wow, it was a little painful when we got to the end, we now know what we want to fix, what we want to do to make us as strong as we can be. I think that's a great process to go through and I can't emphasize enough on employee training, the best systems in place can't stop employees' errors or mistakes. Keeping everyone aware and doing, you know, fake business email compromise, emails to your entire workforce is great. Anybody that clicks on the wrong attachment's got to watch a 20-minute training video. That's a great way to wake everyone up, get them on board and really paying attention because they're your first line of defense.

[Kevin]: Well, cyber insurance application as a risk management tool. I think that's a great place to end and invaluable advice. Laura, thank you so much for joining us on Cyber Sip. I really appreciate it.

[Laura]: Thanks, Kevin. It's been a pleasure.

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