Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 14: "Risky Business: Does Your Law Firm Have 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 the Cyber Sip. Practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

[Kevin]: Hey everyone, welcome back to Cyber Sip. For 95 years now, Arthur J. Gallagher and Company has provided insurance brokerage, risk management, and business consulting services to organizations across the country. Joining us this morning is Laura Zaroski, managing director of Gallagher's law firms practice. Laura draws on her 16 years of experience as a litigator of D&O, E&O, and professional liability claims. And more than a decade on the inside to help law firms place insurance coverage in an increasingly competitive cyber environment. Laura Zaroski, welcome to Cyber Sip.

[Laura Zaroski]: Thank you, Kevin. Glad to be here.

[Kevin]: I'm so excited to have you. And we're going to talk cyber risks facing law firms today. I want to start with the basic question that—I don't know about you, but I get from law firms and professionals that ask me: why do I need this? Why, why did the bad guys target law firms? Why not the major banks and other institutions that have all of the data that everyone's looking for? Why are law firms a target?

[Laura]: Yeah. Law firms aren't really known for having the state-of-the-art security systems. A lot of them are still getting up to speed with what they do need to have in place. I don't want to call law firms "low-hanging fruit," but sometimes they can be much easier targets than the banking, the financial institutions that seem to have had to address this much earlier. So that's one difficult part about being a law firm, is that they really haven't paid much attention to their security for a while. At least many firms haven't. Even the ones that have, you know, there's no foolproof service, you know, foolproof system, as you know. So even if you have put in some of the best and strongest securities, the bad guys can get in and half the bad guys wrote them, wrote those programs, so they know how to crack those programs. So it's really tough even if you have good security in place.

[Kevin]: One of the things that I worry about, and that I wonder if others worry about, are the ethical obligations that come with cybersecurity and the first and most basic ethical duty here in New York, it's the rules of professional conduct, are often modeled on the model rules promulgated by the ABA and Rule 1.1 is competence, that now the comments are not binding. But the comments to Rule 1.1 essentially say that a lawyer has to be competent in the technology the lawyer uses to practice law. And then Rule 1.4, communication, requires the lawyer to talk to the client about that technology, and one would think that that would be enough of a hook to get every law firm across the country interested in robust cyber hygiene. But that's not always the case.

[Laura]: No. You know, those rules are definitely out there. And I think it should be a concern for most practicing lawyers. However, there's not a lot of guidance about exactly what standards meet those rules and which ones don't. So I think lawyers do grapple with that and ones that have basic security think they've met that standard. And, you know, as the case law grows and maybe more cases are filed, I think we'll have our guidance on really how to meet those standards and frankly, more concern from attorneys that they want to make sure they're hitting that correct level of security so they're not subject to any disciplinary-type action.

[Kevin]: Right. So meanwhile, law firms are a target. You mentioned law firms being low-hanging fruit. What are some of the more common claims scenarios that you are seeing at Gallagher?

[Laura]: Well, definitely with the firms we work with, there's always human error. And I throw that out there, even if you have the most robust systems, you still have to have your employees have access and the people that should be having access. And human errors happen. It's as simple as clicking onto the wrong attachment. And we all receive, you know, hundreds of attachments a week. If it looks like it comes from the client and it's something important, you're going to click on it. And that's probably the number one way we see some of these viruses being unleashed in systems. Certainly, claims... the number one thing we're seeing with our law firms are these extortion claims, and we're seeing the demands on those going up tremendously. I think one of our carriers said that they've seen a 518% increase in extortion demands from 2020 to 2021, across their book. So that...those are staggering numbers and certainly put the fear of God in you, which how much money a hacker may be asking for from you. Business e-mail compromise is the same thing as well—huge increases in how much money has been stolen from a lot of our law firms, with some of those spoofed emails, requests from the managing partner to the accounting person to transfer funds, settlement funds going to the wrong person. All those are, again, terrifying, when you know something's gone out the door, it's not coming back. But yet you still owe those settlement funds to the appropriate party.

[Kevin]: Right.

[Laura]: So really tough stuff that some of our firms are experiencing.

[Kevin]: I saw one example of a BEC where the associate received an email at about 7:30 in the morning from the partner saying, I really need you to bring some Amazon gift cards into the conference room right away. And there's a log, there's a click and for the information. And of course, that was an easy fraud to detect and the associate noticed it immediately. But we just had a client, and very successfully resolved the issue. But it was a situation where the risk manager received an email supposedly from the CEO of the company saying, I need a complete rundown of all of our accounts receivables because I want to work on those this weekend. And very dutifully, the risk manager provided a 95-page, single-spaced listing of all...every client of the firm with the AR history, and it turned out to be a threat actor. So the bad guys are getting better at figuring out what causes one to click. And it just... it seems to me like the risk is becoming more significant, particularly when you have so many people working remotely.

[Laura]: Well, definitely the bad guys are more sophisticated and these attacks are more complex. I think, you know, the days of thinking that there's a hacker in his mom's basement with bunny slippers, those days are over. Now you've got sophisticated businesses overseas where, you know, they have meetings just like we do. You know, what worked this week? What isn't working? What extra thing did you do that produced the response you wanted? Layering of these complex crimes. You know, they'll follow up with a phone call to you after sending an email and they'll say on the phone call, you can never be too careful, there's a lot of bad actors out there. I mean, they do this over and over again until they get a certain story that works best. So very sophisticated, hard to detect, and getting even

harder. So that's where the aspect of training really comes in. You know, when you hear these types of stories that we're talking about now, when someone asks you for those gift cards, you think, oh, hold on a second. I heard there are scams where people had to buy gift cards.

[Kevin]: Right?

[Laura]: The awareness, I think, is key right now.

[Kevin]: No, definitely. And I think I think we're getting better at training. But as you say, the threat actors are getting more sophisticated as well. So, we can talk a little bit about cyber hygiene when we talk about insurance applications. But let's suppose, Laura, that I am the risk manager or the managing partner of a mid-sized law firm, 80 to 120 lawyers. And I come to you because I would like to begin the process of placing cyber insurance. Can you walk us through how that process works? Is there an application? What, besides the application, is necessary? Is there any auditing of the firm's physical, electronic, or legal controls? Walk us through that.

[Laura]: Well, I'd say in the old days I used to call it, it's like that old show, "Name This Tune." We had carriers that would ask 30 questions. Then somebody is like, I can do it in 20, I can do it in 10. We got to the point a few years ago or people wanted market share so badly that we had carriers asking four questions and that was the good old days because four questions you get your cyber quote, you're off to the races. That has drastically changed over the last year with all these ransomware attacks, with all the payments that have been made, the business email compromise. We've seen a huge onslaught of claims. So carriers have abruptly changed their underwriting in the way that they're evaluating accounts. So now you're more likely to see that 20-page application. And what are the carriers looking for in that application now? Now they really want to understand what controls you do have in place, and they know what they've seen over their book in the last two years. These are the most common ways that are getting in. So they want to make sure that you've stopped those pathways for the bad guys. The key thing we've seen is this multifactor authentication. Carriers have pretty much put their foot down and said if you don't have MFA in place we're not even considering you. So when I sit down with a client, the first thing we do is we're going to go through the application together. If you don't have multifactor in place, we're going to stop right there and have you put it in place because we're not going to get a single quote for you without it.

[Kevin]: Right.

[Laura]: They're going to ask about patch management. How often do you patch? When do you patch? How quickly? So when those vulnerabilities are discovered, are you taking care of that before somebody can get in, before you get it fixed? And our endpoint detection, looking for that for all the endpoints, all your computers and all the networks you have. Backups is another great question. And they don't want to see just one backup. They want to see multiple versions and different versions. Do you have a backup online? Do you have a backup where you take it offline on a disk? Do you have MFA on those disks? Have you air-gapped it, where you've got one saved here and one saved there? Because they've definitely seen claims where when the backups were infected or they didn't have appropriate backups, then there's no way to restore your system and trying to create it from scratch certainly is almost an insurmountable chore.

[Kevin]: Sure.

[Laura]: That's kind of what we're seeing right now from the carriers: training. Training. Training, as we already touched on. Keeping all your people...I mean, people are your biggest vulnerability. So, you know, every three, six months, if you can let them know what are the new scams we're seeing, what are the new ways they're trying to get in? Once you kind of have that awareness, I think that really

helps your workforce be a little bit more keen and to spot these before it becomes a problem.

[Kevin]: And thinking about the notion of competence. I mean, I remember when I thought MFA was a log-in and a password. I mean and that's part of it is the...what do we really know about some of these safeguards? I think a lot of people out there think, you know, I had a conversation a few months ago with someone not at Barclay Damon, but at a client. And I said, well, do you have MFA? And he said, Oh, yes, we have a log-in and a password for every single person. I said, "Yeah, that's not MFA." So I mean, that's part of the education and training. The folks who are running the organization really need to understand what these safeguards are and what they require. Because if you don't know that, you can't answer the question whether you've effectively implemented them.

[Laura]: Sure. And the thing about lawyers, I mean, they're very good at what they do and they work really hard. But it's definitely a career that doesn't involve any IT whatsoever. So we see a huge gap between like when I deal with legal malpractice...lawyers all understand legal malpractice, we start talking about cyber and asking these questions. Everyone stops and says, no, no, we got to call the tech guy in here. And we've definitely seen now where carriers are looking for and we're trying to get our law firms to understand this isn't going to be a top-down culture of understanding and dealing with security, really understanding what MFA is. Even if you're a lawyer, you still need to start understanding some more the tech side of how things work and what you need to do to be confident in protecting the information you hold for your clients, the information you hold on your employees. So I think we're slowly seeing that change, but that's a big struggle for a lot of lawyers with this. Just this isn't their area of practice and frankly, something they're not that interested in. But I think we've all kind of gone kicking and screaming into 2022 and in many aspects. So I think this cybersecurity in remote working is one of them.

[Kevin]: So, Laura, you mentioned that the application process, I'm curious, have you ever had a situation where you are in the midst of the application process, and you turn to your client and you say, you know what? I don't think it makes sense for us. I think you alluded to it earlier when you're talking about MFA. How common is it for you to be meeting with a client, working on the application, and reaching the conclusion that it just doesn't make sense to even send that risk out into the market because the client's safeguards are not yet up to snuff.

[Laura]: Yeah, definitely we've had that situation. But again, we'll know really the safeguards that you don't have implemented right now, and get you working on those before we're going to take you out to market. Because that's going to make a huge difference when you go out to market on whether anyone's going to write you first of all, and if they are going to write you, what coverage are they going to offer to you? And certainly the most important thing, price, right? You know, you could be paying three times more because you don't have certain security in place.

[Kevin]: Right.

[Laura]: Well, you know, some of these things can be done within a week or two. And some of them are just getting a system, you know, enabling certain systems you've had you just didn't want to use because it's that extra step. So many of these are kind of I won't say quick fixes, but can be done pretty expediently. And then we can get you in a much better place to get much more carriers interested in writing you, in writing with the best terms and the best pricing.

[Kevin]: So you're in that situation where maybe the client is in great shape or maybe the client has some deficits and you spend a few weeks or a few months fixing those deficits, getting the client's application ready to send out into the marketplace. What happens next? How do you decide for which...you know, which carriers to go to, for which clients?

[Laura]: Well, each carrier definitely has their own appetite. There are some carriers that won't write law firms at all. There's carriers that want really large law firms. There's carriers that only want to deal in the small space. Sometimes area of practice can make a difference and even geographical regions. So it's just knowing your markets, knowing who to go to and who is going to write your profile, you know, and that's the broker's job. That's what we're supposed to do, is know the right place and who's going to be most competitive for your account.

[Kevin]: Right. Now, Laura, I see we are close to running out of time, but I want to continue this conversation. Will you come back to us and talk to us about the process of engagement between Gallagher and the carriers, how the policy gets issued, and then your recommendations for law firms?

[Laura]: Oh, happy to do so, Kevin.

[Kevin]: Well, I am grateful and so glad you could join us today. Thank you very much. And thanks to all of you for joining us. We'll be back soon with another episode of Cyber Sip. Stay tuned.

[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.