Barclay Damon Live Presents: The Cyber Sip Podcast

Episode 8: State of the Market – Cybersecurity Insurance, With Kelly Geary

Speakers: Kevin Szczepanski, Barclay Damon and Kelly Geary, National Executive Risk & Cyber Practice Leader, Epic Insurance Brokers & Consultants

[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 this episode of Cyber Sip. I am so excited to have Kelly Geary joining us. Kelly is the national executive risk and cyber practice leader for Epic Insurance Brokers & Consultants. Kelly has been a featured member of the cyber industry for many years. She started when she was 18. And here she is today, and we're going to talk to Kelly about her experience, about how the initial cyber insurance policies came to be, and a little bit more about practical takeaways that we can all benefit from when we're shopping the market for cyber insurance. Kelly, welcome. It is such an honor to have you join us today.

[Kelly Geary]: Thank you so much, Kevin, I'm really excited to be here.

[Kevin]: And I told you offline, and I'll say it for the episode, I think in one sense, I wanted to do this podcast just so I could interview Kelly Geary about cyber. So here it is. Let's talk about the origins of cyber insurance. I've read, I think, a piece in the Chicago Fed that attributes the earliest form to Steven Haase and AIG around about 1997. And that was mainly meant for the folks in Silicon Valley, the tech companies and the dot com bubble. But it wasn't long after that, that you got into the cyber market and you were involved in writing some of the earliest cyber policies, right?

[Kelly]: Yes, that is true. I think that comprehensive cyber insurance policies that we sort of know today really grew up probably more in the early 2000s in response to breach notification laws that started sweeping the country, starting with California in probably 2002 or 2003.

[Kevin]: So when you're sitting down to write these policies, I have done very little of that, but I remember having to write a policy endorsement once and I went online. I found as many different forms I could, of course, nothing looked like what I was supposed to write. How did that process work for you? What sources did you use to sort of create this cyber product?

[Kelly]: It's interesting because initially, like I said, it was really more about—I think the insurance market was trying to provide a solution for companies that were looking to comply with breach notification laws and the costs associated with those in terms of, you know, providing notification in the event of a breach, having some sort of call center set up, if that was required, having, you know, credit monitoring and providing that—that's all financial costs. So initially, what we started looking at mostly really was it was more about drafting coverage around that and trying to provide coverage for that either in endorsement form, so endorsing it to a standalone, say, miscellaneous professional liability policy or something, some

other traditional policy form or trying to create something a little bit more robust and comprehensive. The policies that exist today are incredibly complicated and have, you know, they probably have anywhere from 10 or more insuring agreements, but that's all piled on as the risk has evolved over the years.

[Kevin]: So I'm thinking about that, and I think the last policy I looked at headed insuring agreements "A" through "M," so they're just depending...and every form is different. Let me ask you about that. Let's talk about the difference between what I'm going to call "traditional forms" of insurance that every organization may have familiar with, from GL, property, to professional lines, D&O, E&O, and compare it, if you could, for us with cyber product, which is decidedly less experienced and really still in its infancy.

[Kelly]: I think the complexity comes from the risk, right? So I think traditional forms of insurance and traditional insurance policies are, you know, are kind of crafted around a particular risk that you're trying to address. And those risks that we all know and love, say the property-related risks or professional liability, or employment practices, have, thus far anyway, been pretty predictable, right, with some changes here and there. But the base risk itself hasn't changed or doesn't evolve as rapidly as cyber risk. And I think what you see in a cyber policy is that complexity that multiple different, you know, insuring agreements, trying to address differing risks as they sort of evolve and come up. And so those risks kind of trace and track and run behind advances in technology. So I mean, I was looking at a cyber policy the other day that had over 100 definitions, you know, trying to evaluate a cyber policy with 100 definitions, and like you said, you know, insuring agreements "A" through "M," or apply that to a live claim scenario is incredibly difficult.

[Kevin]: I remember one of the first advising conferences I ever went to. One of the speakers who was very effective and very funny, by the way. He said, it's not comparing cyber policies one to the other is not like comparing apples to apples or even apples to oranges. It's more like apples to hand grenades, because you just ...there's no synchronicity between the policies. Do you think that's going to change in the years to come? Or is this product just so unique and so evolving that it's going to take decades more for it to settle into a standard form?

[Kelly]: I think it might take a little bit longer. I thought, you know, if you had asked me this question five years ago, I probably would have said, yeah, it'll...it's coming, the standardization is coming. I think there's a bit more standardization in terms of the coverage being offered. So in most of the policies out there today, you're seeing the same types of coverage offered. So you're seeing third party liability, you're seeing regulatory, you see cyber extortion coverage, you see, you know, business interruption. And so the key buckets of coverage are all there. But the scope of coverage varies so greatly because you have all of these different approaches in terms of definitions, and exclusions, and terminology.

[Kevin]: So let's drill down a little bit into those buckets, Kelly, so you've got an organization out there, they know they have GL, they have property, they have D&O, E&O, EPL, but they don't have a cyber insurance policy, and they're trying to decide whether they need one. What types of risks are we talking about and what coverages does this cyber liability policy afford? I shouldn't say "liability" because there's first party and third party coverage. Can you talk to us a little bit about that?

[Kelly]: Sure, sure. So most comprehensive cyber policies, you know, as you indicate, provide some third party liability coverage and then a bunch of other first party coverages. When an organization is hit with a cyber attack, the first thing that they need usually is, aside from some legal advice and breach counsel to sort of help them manage through the event, they need a computer forensic firm to come in and try to figure out what happened and stop the bleeding and control the environment a bit. And that's costly. So, so breach response costs in general are the key first party coverage that you find in every standalone cyber policy—that I've seen anyway. So the breach response costs will include costs

associated with hiring a computer forensic firm, hiring a lawyer, a breach counsel, a privacy lawyer that's going to help sort of create that attorney-client privilege so that the incident is contained, at least from the standpoint of potential liability in the future and just guide the organization through the response. So you may need if it's a ransomware attack, you may need a ransomware negotiator. That cost would be factored into that, you know, that coverage you have call center, breach notification costs. All of that stuff is in the first party. In terms of, you know, ransomware that that tends to be obviously the big ticket item these days. There is cyber extortion coverage in all of these policies. But it does vary widely in terms of the amount of coverage that's being offered. Deductibles, sub-limits, co-insurance. By and large, most of these policies will provide coverage for the ransom negotiator, for costs associated with sort of dealing with the event, and also payment of the ransom so long as it is legally permitted, and all of that coverage is in the first party. The other big element of coverage in the first party sense is business interruption. All businesses rely so heavily on technology today if your systems go down, chances are you're going to sustain some sort of business income loss and that would be also covered in in a cyber policy.

[Kevin]: And that's the first thing when we have a client come to us with a ransomware attack. The first thing they say is how can I get back to running? What am I going to do to continue my operations when my data has been locked and all I seem to be able to do is pay ransom to get it back? I want to come back and talk to you about ransomware, but you mentioned some of the complexities and the different layers of cyber insurance. And I know, of course, Epic is one of the largest and leading professional lines brokers in the country. A lot of organizations, small to medium size, have local and regional brokers. One of the things that strikes me, though, about this product is that, unlike general liability or property, there really is an expertise that cyber insurance brokers possess that I think the rest of the market is slowly catching up with, but doesn't necessarily have. We know many strong brokers—but talk about that and the importance of having an experienced broker who knows this product and can help the organization compare apples to oranges.

[Kelly]: Right. No, and you're absolutely right, and I think that the market has evolved quite a bit in the last couple of years in particular. And we are starting to build a talent base. But I am concerned and have been for a long time about not only brokers and operating in this space, but carriers with claims professionals that maybe are not that involved in cyber or handling cyber claims and other claims at the same time. You know, this is just been a product that has evolved very, very quickly. It is one of those, you know, as I mentioned before, the risk itself evolves so rapidly that unless you are immersed in it—so whether you're a broker, a claims professional, a lawyer, any... a computer forensic firm, anyone, unless you're literally immersed in this product and this risk, you're probably going to be behind. Right? And I think that the individuals, again, any kind of side of the fence there, whether it's a broker, claims professional, lawyer, that dabble in cyber, it's very I think that's very dangerous, because it does evolve very, very quickly. It is very complicated. So one of the things that we do when we're evaluating a cyber market for our clients is we look very deeply into the claims expertise and the underwriting expertise. There are a lot of cyber underwriters right now because the demand is so high, the carriers are hiring a lot of cyber underwriters, cyber claims professionals. Same thing with cyber brokers getting them all in. There's not that many people that have a lot of experience with the product. So you see a wide range of expertise.

[Kevin]: You talked about the expertise and you mentioned underwriting. So I want to go there now and we've got a little bit of time left. I want to talk about that because what we all hear is that the market is hardening. So what does that mean for those of us that don't know what that phrase means, and how has it affected how the carriers underwrite the cyber risks?

[Kelly]: Yeah, it's a great question, Kevin, so...and I kind of refer to maybe about 15 to 18 months ago. Up until about 15 to 18 months ago, I refer to cyber as...the cyber market was like the glory days, right? It was the coverage. I mean, the demand was far below the supply. You had tons and tons of markets out there writing, the insurance coverage was super negotiable. You could pretty much get whatever you wanted, added, or changed to the policy. The prices were super, super low and underwriting was almost an afterthought.

[Kevin]: It really was.

[Kelly]: It was like I had markets coming to me, you know, kind of, you know, arguing about, you know, "Well, I can do this, I can do this with two bits of information." "I can do this with three bits of information." And really, you could get a cyber quote and a cyber policy with very minimal information. Your, your name, your website, whether or not you had any claims. And that would pretty much have been enough. And the market did harden, so it did tighten up. It got a lot tougher in the last about 15 to 18 months ago, where all of a sudden now we are, we completely flipped the switch and prices are very, very high. Capacity is restricting. Markets are pulling back on the limits they want to give and they want to offer. They're pulling back in certain industry classes that they feel are too risky. Coverage is not negotiable anymore at all.

[Kevin]: When you say the terms are non-negotiable, you about limits, things like certain insuring agreements.

[Kelly]: Yeah. So, so definitely limits. I mean, you pretty much can only get $5 million. So we've had we had a lot of large organizations that had towers of insurance of up to $70 million that we can't even get that for. But if you had a $10 million policy last year, you're going to have to have two carriers on your... in order to get $10 million this year because most, most markets will only offer $5 million now. And most markets are sub-limiting ransomware, so they may give you a $5 million dollar insurance policy, but they're going to say you only get a million dollars for ransomware-related coverage, which is the big risk.

[Kevin]: Significant cutback. So if your we've got a couple of minutes left, so let's...beg the question that if it the market is tightening, what can an organization do to maximize their chances of getting a cyber insurance policy if they don't already have one, or even maintaining or renewing the existing policy that they have in place?

[Kelly]: Well, the underwriting, back to your one of your initial questions is the underwriting has changed drastically. There, you know, it's much more in depth and detail and technical underwriting today than it was 18 months ago. There are certain network security controls that an organization must have in place in order to even get the insurance policies. So multifactor authentication, demonstrating network segregation, endpoint detection and response—there are a number of different, I would say there's probably about 10 to 12, and they sort of evolve and change a little bit and vary by market, but there are a handful of network security controls that if you don't have, you're not going to get a policy at all.

[Kevin]: It has changed dramatically. We're out of time for this episode. We did not get a chance to talk about ransomware or coverage issues, but will you come back and talk to us about those in a future episode?

[Kelly]: Of course.

[Kevin]: Thank you so much. Really appreciate your joining us today, and thanks to all of you for joining us. We'll be back in two weeks with another episode of Cyber Sip.

[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 opinions. 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.