
*Barclay Damon Live Presents: The Cyber Sip Podcast*

**Episode 13: "Three Secrets about Cyber 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]:** Hey everyone, welcome back to another episode of Cyber Sip. I am proud to be joined again by Kelly Geary. Kelly is the national executive risk and cyber practice leader with Epic Brokers and Consultants. Welcome back to Cyber Sip, Kelly.

**[Kelly Geary]:** Thank you, Kevin. Glad to be here.

**[Kevin]:** Thank you. And our viewers do not know how close in time we've actually visited between the first and second episodes. But I welcome you back and really appreciate your joining us. The last time we talked about some of the basics of cyber insurance, we did not get a chance to talk about some of the trends and coverage issues that have come up. So I thought we would have you back to talk about those now. And I want to get right to it. I have heard you talk about a few of these issues before, and I thought our listeners and viewers would really enjoy hearing from you directly. One of them you talked about on the "She Said/He Said" podcast, I have to give this a plug. This is the Daniels husband-and-wife, right? It's Justin and Jodi Daniels. And they had a terrific podcast. [Note: The podcast title is She Said Privacy/He Said Security.] You visited them for quite a while and you were talking about how important the policy definitions are in a cyber insurance policy. And one of the most important definitions that can create coverage issues today is the definition of "computer network" or "computer system." Let's talk about that now. What is it and why is that a potential issue we should all be worried about?

**[Kelly]:** So, yeah, so, you know, in my mind when I think about cyber insurance policies, that is the heart and soul of the coverage, right? Because everything that flow, all of the coverage really that flows in that in that policy comes from or connects back to in some way the definition of "computer system" or "computer network" or whatever the term is.

**[Kevin]:** Right. Right.

**[Kelly]:** So one of the things that that I advise our clients on and we try to do with our clients is really say, let's look at the definition of "computer system" or "computer network" in this policy and let's sit down with your IT professional and let's make sure that what you think your computer system is, is the same. And if it's not, let's tweak it or let's try to change that definition so that we make sure that it's as broad as it needs to be from a coverage standpoint.

**[Kevin]:** And one of the issues that it implicates is BYOD, "bring your own devices" for remote work, right? So more and more of us are working remotely. I've been largely working remotely since April of 2020. How does the definition of computer system affect potential coverage for employers that have employees working remotely or perhaps with their own devices?

**[Kelly]:** So pre-pandemic, there, most cyber insurance policies, those definitions had "owned and operated" wording within the core definition, which basically meant if you were a company and you issued, you know, iPhones or laptops to your employees, so you owned them, you just gave them to your employees to use for work purposes, then that would be fine. You would be within the scope of the definition because you, as the named insured, own the devices and you gave it to your employees to use. But the problem was, is even before the pandemic, many organizations had started to shift to "bring your own device." So these were employee-owned devices that were able to access the network of the named insured of the company. So you really needed to tweak those definitions in order to make sure if you were an organization that allowed your employees to bring their own device, you need to make sure that that actually fit within the definition of your cyber insurance policy. And it wasn't always the case. I will say that when the pandemic hit and we were all pushed into largely remote work environment very abruptly, a lot of the cyber markets were responding affirmatively and issuing endorsements or changes in wording so that they could address that. And not all, but some.

**[Kevin]:** That you say "not all." So to some degree, this issue, this risk is still out there.

**[Kelly]:** It absolutely is. I was looking at a cyber insurance policy for one of our clients just the other day where there were amendments to different definitions to address the bring your own device, but not to the core definition of computer system, which I view as being very intentional on the part of the of the carrier. They intentionally did not want to broaden the definition of computer system. So you have to be very careful because you can see it amended in different definitions. But if it's not actually the actual definition of "computer system" or network, you got to be careful.

**[Kevin]:** You know, this is so important. And it reminds me of something I heard you say at a presentation long ago, and that is you really need to have an industry professional help you walk through these policy forms, because I think sometimes people will look at their policy and they'll see an endorsement that says "cyber" and they will think that it's adding cyber coverage when in reality it's either an exclusion on its face, or it is an endorsement that is making explicit the limited nature of whatever cyber coverage there is. So if you don't have an insurance professional reading that with you and explaining, you know, hey, this is not cyber coverage, this is a limitation to your existing coverage, you can have trouble that you don't find out about until you get that cyber protection, right?

**[Kelly]:** 100%. And I think that the other thing that we've seen in the marketplace in the last say, again, maybe 18 to 24 months is a movement within the insurance market as a whole—so not just cyber—the insurance market as a whole to try to address cyber risk and try to contain the risk within traditional and traditional lines insurance. So a property policy, an employment practice policy, and a lawyer's professional or an E&O policy. So you're starting to see either affirmative exclusions being added to these products or affirmative coverage. So you actually oftentimes and I've seen this with some of our clients, oftentimes there are... there's coverage in two places, but they're not coordinated...

**[Kevin]:** Right.

**[Kelly]:** So then you have two carriers when an event happens and you have two carriers sort of pointing the finger at each other in terms of who should step up first. And you see that a lot in, you know, and cyber, especially actually with, you know, lawyers, accountants, where the nature of your business is to keep information confidential. That's your professional service. And so the possibility for overlap

with a cyber policy is high.

**[Kevin]:** Right. Talking about the overlap between malpractice insurance and a cyber liability coverage. Absolutely. That leads me to a question I wanted to ask you about, which is the... does the overlap potential for overlap caution in favor of having the same carrier, ensuring multiple risks? So there... I think there's pros and cons, and I wanted to ask you about that. So one of the benefits I see to that is that if you have the same carrier on both your professional malpractice and cyber liability coverage, they may be pointing the finger at each other internally, but presumably one of those policies will inevitably respond. It's just a matter of figuring out which one. When you have two different carriers, the finger pointing can be a bit more difficult to navigate.

**[Kelly]:** It can. I think one of the other things that becomes challenging is whether or not the same carrier is willing to write both.

**[Kevin]:** Right.

**[Kelly]:** So the carriers have been very nervous about systemic risk and sort of controlling that to some extent or to the extent that they can. So there are a number of carriers that don't want to be on both sides of that fence, or if they are, they will add a tie-in limits endorsement. So where they're saying, look, if both of these trigger, only one limit applies. So it's hard. I think what you see most often is buckets of coverage. So you see that your cyber insurance would be your main source of coverage. And then you might have, you know, an E&O policy, an affirmative grant of $25,000 or something like that a bucket of small and you know, you have to, number one, recognize that it's there. And number two, understand what definitions and the scope of coverage exist in that, because oftentimes it's very different than what you have in your cyber policy. So they both might not trigger at the same time. But I'd say the most common overlap, aside from a lawyer's professional, for example, would be on a commercial crime policy. So you definitely see overlap there. And in the past it's been with K&R policies. So kidnap/ransom policies, up until recently, provided cyber extortion coverage. So I've handled a number of claims where there was, you know, full on cyber insurance, cyber extortion coverage and a kidnap ransom policy. And in their cyber policy. But they weren't coordinating so there was arguing still between carriers.

**[Kevin]:** And I think it just speaks to the importance of having an insurance broker there to make those arguments to the carriers. Because at Epic and our other broker friends, you have relationships with the carriers and can more easily navigate those thickets and have that conversation to coordinate coverage. And you're in a better position to do it than our clients and organizations are.

**[Kelly]:** Yeah. I mean, I think, you know, and I've always I'm a bit of an insurance geek. I think, you know, that, Kevin.

**[Kevin]:** And a very effective one as well.

**[Kelly]:** But I think I truly believe that today policy wording is more important than it ever has been, especially as respect to cyber risk. But I think that's true across the board, because I think the insurance industry, again, as a whole is shifting to try to address this very, very dynamic risk that permeates every organization at every size and every geography. There's... it's you know, it's indiscriminate, really. And it's blurring the lines between it among all insurance products. So the policy wording and having a good coverage attorney look at stuff with you or advise you or a good broker is super, super important.

**[Kevin]:** And we're talking about this overlap. It brings up the concept of "silent cyber coverage." And I've heard you talk about that before. It's hot today. There's a decision out of the New Jersey court that essentially held that Merck had suffered a cyber incident, turned to its insurance carriers for

coverage, and many of the carriers disclaimed on the basis of a war exclusion in their policies. And the argument was this cyber incident was attributable to a nation state. It was Russia. And although the Kremlin, of course, denied it, US and UK officials had plainly stated this was an act of the Russian government. And the carriers looked at this and said, well, it's not a physical war, but cyber warfare is a well-known concept. They tried to disclaim under their war exclusion, and the court said, no, the war exclusion is limited to actual physical hostilities, it was never understood to be an exclusion that extended to modern cyber warfare. So talk to us a little bit about that and the broader concept of this cyber ...silent cyber insurance and how policyholders are trying to locate cyber coverage in policies that may never have been written to provide it.

**[Kelly]:** Yeah. I mean, you know, the insurance industry really likes to keep risks in their lanes. Right. So if it's an employment-related risk, they want it to sit right in an employment practice, liability policy, if it's a legal, you know, negligence in connection with the provision of legal advice or accounting. They want it to sit right in that, you know, they don't like when it when there's a blurring of those lanes and cyber risk just does that. And so I think that, you know, the Merck decision is an interesting one. I think the war exclusion in and of itself is fascinating because it was probably written 100 years ago when, you know, hostilities were different, right. And I think in that Merck decision, it was in a property policy that they were trying to sort of get some business interruption coverage associated with the NotPetya attack back in 2017 I think. And you know as standalone cyber policies have cyber terrorism carve-backs to the war exclusion, so almost all policies have a war like cyber insurance specifically has carve-backs to that war exclusion. But here's another example of the devil's in the details, right? Some of the carve-backs in some of these policies are much more narrow than others. So you may see you may scan down your policy and say, yeah, there's the war exclusion. And it says, except for cyber terrorism, but you have to go look at the definition of "cyber terrorism." And in some policies, the definition is "only if the attack is directed at the named insured."

**[Kevin]:** Which is rarely the case.

**[Kelly]:** Very rare that you would have an act of war, or act of cyber terrorism, on a company.

**[Kevin]:** Right.

**[Kelly]:** Right. So, you know, the NotPetya attack was what you would consider to be a generally distributed attack that just happened to impact Merck. Right. And impact a lot of companies. So you got to be careful of that wording. And we try to we try to change that so that it's not directed at and it would apply to anything that impacts the named insured. But. It's hard sometimes you got to again, devil's in the detail when it comes to coverage.

**[Kevin]:** Yes. And just again, augers in favor of having an insurance professional up front, sit with you, walk through these forms side by side and explain what might and might not be covered so that you can make a prudent choice between competing insurance forms or decide whether you want to purchase the coverage in the first place. We could do a whole episode on ransomware. We're not going to do that today, but in the time we have left, Kelly, I wanted to turn to one other coverage issue, and that is in the ransomware context, because we know that OFAC, the Office of Foreign Assets Control, has implicated the potential ransomware coverage that many organizations who have cyber coverage thought they purchased. It was interesting. I was listening to an interview that you did on another podcast about I think it was a year and a half ago, and you were asked, what do you think's going to happen? Is there going to be a narrowing of insurance coverage based on OFAC's, increasing enforcement activity? I should stop to note OFAC is a unit of the US Treasury Department. They are a financial intelligence and enforcement agency. And one of the things OFAC has been doing in the last 6 to 12 months is really clamping down on the ability of organizations to pay ransom to threat actors, to the illicit organizations that are on OFAC's sanctions lists. So I wanted to ask you about that and

how that implicates ransomware coverage. Is that... are you seeing that as an emerging issue among your clients now?

**[Kelly]:** It definitely is. I mean, it's something that none of the insurance policies will provide coverage for a or a reimburse, a ransom event, a reimburse, a policyholder for ransom paid to to an entity or an individual on the OFAC list.

**[Kevin]:** They will include... there's an exclusion in most of it.

**[Kelly]:** And even if there isn't an exclusion, they can't pay. It would be an illegal payment.

**[Kevin]:** Right.

**[Kelly]:** So they can't pay. And I think the biggest issue is because, you know, as you pointed out, Kevin, OFAC is focusing on cyber-crime right now and cybercriminals in particular. And so who they put on that list is evolving to some extent, right? And we had a client that had a ransomware event. Paid the ransom. Typically when you're in that kind of environment where you're negotiating with the ransom, with the with the cybercriminals in terms of what the ransom is going to, you know, what ransom will be paid, what amount. You have a ransom negotiator. They are typically going to run the name of the ransomware or, you know, variant or the criminals or the individuals, whoever's being paid. They'll run that through the OFAC list to make sure they're not on the list before they the payment is made, right? So in this instance, they ran the name. It was not on the OFAC list. The policyholder paid the ransom, $2 million. And then they went about the business of regaining control of their network and getting themselves back up and running. Ransomware coverage, typically in a cyber policy is a reimbursement covering. You need to pay and then they will reimburse you, right? So two months go by and they submit all of the information they need to try to get reimbursement for the payment of ransom...

**[Kevin]:** So let me stop you there. You hold that thought. So here we are right now, just to set the table, there's a ransomware incident. The policyholder decides to pay the ransom. The insurance company doesn't advance the $2 million. The policyholder has to pay it and then seek reimbursement from the insurance company. So the ransom is paid. So far, so good. The policyholder assumes that it's going to be reimbursed for this $2 million payment. Forgive me. I just I just wanted to set that up. So then what happens?

**[Kelly]:** Then they submit all of the information they need to get their money back from the insurance carrier. And I will say that at the time the ransom was paid, the insurance carrier was involved. So they were involved from a high level. They knew the payment was being made. They knew the OFAC check was done, and it was clear. But two months go by. And that entity was added to the OFAC list.

**[Kevin]:** Right.

**[Kelly]:** So when the insured when the policyholder turned around two months later and said, I want my $2 million back. The insurance carrier said, we can't pay it. We can't pay it. And so, you know, it's a cautionary tale really in terms of, you know, it could change at any moment. It is a reimbursement coverage. So one of the things that we advise our clients to do is to seek reimbursement almost immediately.

**[Kevin]:** Right.

**[Kelly]:** Right. And the and the problem with that is, you know, a ransomware attack and recovering from a ransomware attack, it is a true crisis event for any firm of any sort, any company, regardless of size. There's a lot going on. You're trying to get yourself back up and running so you sort of make the

payment and then you're... that's what typically people do. And then they kind of say, all right, let me let me finish getting up and running, and then we'll see. Then we'll deal with the insurance. When it comes to ransom payments specifically, you got to get that money back right away. You got to turn around almost the next day and submit the proof of loss to the insurance carrier and try to get that money back as soon as you can, because you do have the activity from the federal government where they're like, we've got to figure out how to how to get rid of ransomware as a problem, so we're going to start adding entities and variants onto the OFAC list. You got to watch it.

**[Kevin]:** And of course, there's the separate issue which we can ...we could talk about another time about, whether... the moral hazard associated with paying ransomware. But let me ask you this. So we're having this this discussion about this cautionary tale. And it begs the question, which we've heard from some of our clients when we talk about whether they should make a ransomware payment. Explain the OFAC issues, the potential that they won't be reimbursed. And inevitably, a client or two will turn to us and say, well, then what is the benefit of this ransomware coverage if I can't be reimbursed for the ransomware payment? And I wanted to ask you about that in our remaining time, because I think the answer is there is a significant benefit to the coverage, even if you don't get reimbursed for a ransom payment, even if you decide not to pay the ransom. Can you talk to us a little bit about that?

**[Kelly]:** So a standalone cyber insurance policy has so many other insuring agreements and coverage parts that would kick in to help defray some of the financial impacts of a ransomware attack. First and foremost, of course, is the computer forensics just to address the issue at the outset, to, you know, assist during the course of the negotiations before you even were to get anything back. And then also, obviously, the recovery, data restoration, network, getting your network back up and running regardless of whether or not you pay the ransom. You also will have coverage for regulatory investigations in case there are any sort of follow-on regulatory investigations, any follow-on civil actions that arise in connection with the ransomware attack. And there's also, of course, business interruption coverage. The business interruption coverage is hugely important. And, you know, most organizations are going to be down about 7 to 10 days, if not longer, just before they're completely back up and running. They may get back up and running partially, but they're not going to be 100% for a while. So that business interruption coverage is key as well.

**[Kevin]:** Yeah. So the coverage is invaluable even if you're not going to be able to pay the ransom. I think that's really helpful. So, Kelly, we're out of time, but I want to close with one question, and we're always encouraged to ask our clients and the people that we work closely with: What keeps you up at night as a way of really cutting to the heart of the issues of the day? So I want to turn that on you. What keeps you and your colleagues at Epic up at night when it comes to evaluating cyber risks for your clients?

**[Kelly]:** I think the biggest challenge really is that it evolves so quickly. It's hard to give any kind of predictability, you know, any kind of comfort to a client in terms of predictability and say if you do these things or if you have this particular policy in place and you do these five things, everything will be okay. It just is such an incredibly dynamic risk that it's hard to predict. And so that's challenging.

**[Kevin]:** Kelly Geary, national executive risk and cyber practice leader for Epic. Thank you so much for joining us. I really enjoyed talking to you and I hope you'll come back and see us again sometime.

**[Kelly]:** Absolutely. Kevin, I loved it.

**[Kevin]:** Thanks. Thank you. And thanks to all of you. 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 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.