CARLTON FIELDS

Hot Topics in Cyber Coverage [PODCAST]

CYBERSECURITY AND PRIVACY | LIFE, ANNUITY, AND RETIREMENT LITIGATION | FINANCIAL SERVICES REGULATORY | PROPERTY & CASUALTY INSURANCE | OCTOBER 20, 2015

John C. Pitblado

Joseph W. Swanson

Insurers face a potential double whammy when it comes to cybersecurity threats. Like other companies, they must be vigilant about protecting the sensitive data they collect and store from hacks and breaches. On the other hand, insurers also are responsible for paying for claims when a breach occurs. Insurers are scrambling to craft new coverages in the wake of new risks and liabilities, while insurance regulators are scrambling to implement enhanced regulations requiring insurers to meet heightened cybersecurity standards.

Insurance litigation attorney John Pitblado and former criminal Assistant U.S. Attorney and Computer Hacking and Intellectual Property prosecutor Joseph Swanson discuss hot topics in cyber coverage and the business of cyber insurance in this *Carlton Fields on Cyber* podcast.

Use the player above or listen on SoundCloud.

TRANSCRIPT

Joe: Thank you, Christina. It's great to be here, and this is a very timely topic, and it's something that is in the news daily. Not just cybersecurity and the various risks that have gained attention, whether it be hacks, rogue employees, lost devices, things of that sort, but also what companies are doing to mitigate those risks, and in particular, what they're doing with regard to cyber insurance. And so, John, I think this will be a topic of great interest to our listeners and I know we have a number of topics to cover, but I wanted to start with some basics first. And in that regard, I wondered if you might just explain what we mean when we talk about cyber insurance.

John: Sure, yeah. Thanks, Joe, and thank you, Christina. So cyber insurance is a specialized form of commercial coverage designed to insure against losses associated generally with network security issues. It has, in fact, existed for quite a while in manuscripted forms, but it has come to some prominence recently. As you noted, data privacy has become a paramount

public concern, given the constant drumbeat we're seeing of these massive data breaches.

So it has now become a standardized product more so than it had been. It is the Insurance Services Office, ISO, which writes standardized coverage language, has included now some cybersecurity coverage language as well as cybersecurity type exclusions in policies that are not meant to respond to them. So it's really become its own form of insurance separate and distinct from other insurance that is typical, commercial general liability or D&O and E&O policies that we're used to.

Joe: And I've read somewhere, John, that cyber insurance premiums last year, 2014, were approximately $2 billion as compared to just $600,000 in 2010. That's obviously just a massive growth in premiums paid for this type of insurance. Why is this such a hot topic with such incredible growth in premiums?

John: I would say, in a word, Joe, it's fear. And in 2013, Sony suffered a coverage decision in New York court arising from its PlayStation data breach, which was pretty well-publicized. PlayStation is a video game console, and Sony ended up in a class action suit brought up by consumers of its PlayStation devices, whose data was hacked and their account information was hacked and compromised.

And it was a much-watched case because the exposure was massive. And ultimately the insurer won on a summary judgment, no obligation to cover. That was in 2013, and there was, really since then, that case and others like it, we've seen folks scrambling to make sure that they have their cyber insurance house in order, that they have policies that are specially designed to respond to those types of things rather than counting on their old CGL policies to respond.

So these big data breaches have probably fueled the massive growth that we're seeing, and I think many industry watchers are expecting to see it to continue to grow fairly astronomically. I saw some estimates by PricewaterhouseCoopers. They pegged the premiums maybe four, five years down the line as doubling again to maybe five billion, maybe as much as seven-and-a-half billion by 2020 as the market starts to settle down, but it's looking like growth city at present. So on the business side, for insurers, for property casualty insurers writing it, cybersecurity has been and will continue to be a boon.

Joe: And for those insurers, and I know that you spend much of your day representing them in a variety of matters. It seems that they ought to be interested, and are in fact interested in this topic for a variety of reasons, a variety of angles, and I think we were going to cover a few of those today. Just briefly, what are those and what do you anticipate we cover here in this podcast?

John: Well, there are sort of three things I have in mind here, and one of them is something that maybe isn't considered often enough, but it has become a very hot topic, and that is cybersecurity as a regulatory issue. Departments of Insurance are looking very closely at insurer behavior from various angles. And of course, coverage, as we see folks changing from relying on their old CGL policies and the kind of coverage litigation that we've seen arising under policies that weren't necessarily designed to cover these types of losses to the new policies that are specifically designed for these types of losses and what coverage issues will arise there.

So...and really, insurers are at the forefront, and they are going to push the entire cybersecurity landscape forward because they're incentivized to. They want to bring claims costs down. They want more businesses to purchase cybersecurity coverage. And businesses are more and more interested in purchasing cybersecurity coverage, and the end result is going to be a benefit for consumers, whose data is ultimately going to be more secure.

So they really...because they are paying the claims as well as are subjects to cybersecurity regulation themselves, insurers, and particularly property casualty insurers, are really at the forefront here.

Joe: John, let's focus on that first topic you mentioned, which was the regulatory issues. What regulators in particular are focused on insurers? Who's really leading the charge in that regard?

John: So state insurance departments, first and foremost, I would say. And a sort of interesting anecdote as to how, I don't want to say stumbled on the topic, but became much more interested in it. I was attending one of these typical rubber chicken Bar Association-type dinners and I was intrigued, however, by a presentation by Anne Melissa Dowling, who was then the Acting Commissioner at the Connecticut Insurance Department. And she was...really her whole presentation was about cybersecurity and how this is the A - number one issue for regulators and they're going to be taking very close look at insurers.

And it wasn't the speech I was expecting. I thought it was very interesting. Our colleague Bert Helfand and I were there and spoke to her afterwards and managed to score a sit-down with her a few weeks later at the Department, and she brought

with her one of her chief technology folks. And we just had a wide-ranging discussion about where she thinks this is headed. She noted that...and this was late last year in 2014, that the NAIC, which is the National Association of Insurance Commissioners, sort of a federated group of insurance commissioners that meet and create model laws and do things like that, created, right around that time, a cybersecurity task force.

So it was on their radar. And the task force was created I think in October or November of last year. And in fact, Commissioner Dowling ended up being on that task force. She's now the Commissioner in Illinois, and I think Connecticut's Commissioner actually is on the task force as well. But they are focused on a number of issues.

I think, first and foremost, are issues surrounding insurer's protection of consumer data. And this is particularly important for insurers because they are a big player in the world of big data and housing electronic data. They're big companies. They're some of the biggest companies, and they have massive amounts of data, and they also tend to have some of the more sensitive types of data housed, everything from personal health information, your child's X-rays, for example. Maybe sitting in a computer network at some health insurer, your personal financial records. Maybe housed with your life insurer - for that matter, your auto insurer may have real-time analytics coming from a telematics device installed in your vehicle to determine your premium costs.

So it's a massive set of data that these companies are managing. And again, some of the most sensitive personal data. So the commissioners are very focused on insuring that that data is secure and that there are best practices in place. And it was an interesting conversation. We asked, what are you looking for? What types of things are you asking them at this point? Do you have a model list of best practices?

And they, at that point, maybe didn't quite yet. The NAIC is developing them, but it was an interesting conversation. She said, "Hey, are these companies hiring hackers?" That's an interesting concept. Not all hackers are bad, and if you want to stop hackers, the best way to figure out how to do that is to ask hackers.

And I said, "Well, are you employing hackers because, of course, the Department of Insurance is housing massive amounts of consumer data as well." And she thought that was a very interesting question, and a kind of turnaround back on her. And that thought sparked in me, I should probably know more about our own cybersecurity policies at our law firm and started looking at that, looking at our cybersecurity coverage, which we have. I'm sure most law firms do now.

So it's a hot issue for them. And another issue is solvency. And that's always a big issue for Departments of Insurance, is ensuring that insurance companies under their watch don't go under. Well, these claims are so massive that it could present real issues, and they want to make sure that they're not underwriting more than they can handle.

So those are some of the main regulatory issues that the NAIC and individual departments are looking at.

Joe: And John, given that regulatory focus, which I guess is two-pronged as you've outlined it. One, for the insurers as potential victims and also as entities that may have these solvency issues, what, given that reality, can insurers expect going forward from the relevant state insurance commissioners and other players in this area like the NAIC?

John: Well, the Anthem breach is a good example. They're kind of our canary in the coal mine on this. They were the first real big slash news of an insurer suffering a data breach. It was extremely well-publicized. You couldn't open a newspaper without reading news about Anthem over the last months. State regulators, I would say, swarmed. I think New York and California were tripping over each other trying to take the lead in a multi-state market conduct exam, which was kicked off very quickly ,within I think a month or so of the breach.

Ultimately Indiana took the lead role there, joined by several other state commissioners in conducting a multi-state market conduct exam. And not only did they face that prospect of a fairly costly scrutiny process from insurance regulators, but they were also being investigated, the whole entire breach was investigated by the FBI, which recently concluded its investigation.

And it was fairly interesting. It revealed that the hack was not a hacker-type operation looking to score financial data for some type of financial fraud. Rather it was a bad actor-type nation-state hack that was for the purpose of obtaining the sensitive information, fingerprints and other things. So insurers can expect that if they suffer a breach themselves, the regulators will come riding, and first among them will certainly be the state insurance commissioners.

Joe: And given...you mentioned in that discussion about the regulatory interests, that one of the concerns is that these companies may face solvency issues just given the sizes of the claims that are often made when an event like this happens

for an insured. Can you talk a little bit about what insurers are doing to address that concern, and in particular, what some of the coverage issues are that have come to the fore thus far in cyber insurance?

John: Yeah, sure. Well, Anthem, again, is an example. The costs there were astronomical, in the hundreds of millions and counting, reporting at the...actually at the last NAIC cybersecurity task force meeting, included reporting from the GC at Anthem on the breach, and they did in fact have insurance in place. The first layer insurer, I think it was a $10 or $20 million layer, responded and covered. And they are, at present, I think pursuing the rest of the coverage up a tower of insurance.

Often companies with that type of exposure that Anthem has purchases towers of coverage, which include a primary policy of $10 or maybe $20 million in liability coverage, with then additional excess policies sort of stacked on top, which can result in towers of coverage that cover up to $100 million. So, so far no coverage issue out of the Anthem breach, but we have seen some sort of changes, I would say, in the coverage landscape.

Joe: So John, you mentioned, in talking about the regulatory issues, that one concern among regulators for the regulated entity insurance companies is that there are solvency issues given the size of the claims and the exposure we're talking about in these cases. Presumably one of the ways that the insurers are addressing that is to make coverage determinations, and I wonder if there are some trends that you've seen emerge in that area in particular.

John: I think what we're seeing now is a sort of shift from what I'll call first wave litigation, coverage litigation that is a sort of hodgepodge of cases addressing claims for, for example, data breaches or other cybersecurity issues, but made three, four years ago when these policies were not commonplace. And so the claims were made under, for example, a CGL policy, a commercial general liability policy or a D&O policy.

So in those types of situations, you're going to see, I don't know, growing pains for lack of a better term, as an industry adapts. It's a common trend in the world of insurance. I would liken it to "the 1970s" when new environmental regulations where created, creating massive new exposures for regulated entities. And when claims came in predictably, they would go to their insurers, and their insurers had written coverage that didn't have these new exposures in mind.

And so there was a lot of coverage litigation testing those old policies. And ultimately insurers responded by crafting a pollution exclusion, which was...It's actually called the absolute pollution exclusion. I think it's called the absolute, and it's in all bold and caps, pollution exclusion, to make very clear that those old policies were not meant to cover that new liability.

And in its place, new opportunity was created for business, for property casualty carriers to create a pollution-only type coverage. So that's when environmental pollution-type policies were created, standalone policies that are meant to work together with a CGL policy. So if you're a regulated entity that is in the business where you could be a polluter, you're going to have both the CGL and now a pollution liability policy.

And then those new policies get tested. Coverage questions inevitably arise, and then the coverage scene sort of normalizes and insurers and regulated entities have a good idea of what's covered and what they're purchasing. So we're seeing the shift now, I would say with cybersecurity in similar way. Companies have come to realize, like I mentioned with the Sony hack, of the PlayStation hack that there was no coverage for Sony under its CGL policy. And I think that sent some shockwaves back in 2013.

So there are few other cases. In fact, the Sony case was particularly unhelpful because it was a simple postcard bench decision. So there was no real analysis of the coverage issue there. We saw some other coverage cases that were interesting. I actually attended a very interesting oral argument here at the Connecticut Supreme Court on a much-watched case, which also involved a CGL policy. And ultimately the Connecticut court held it wasn't covered. It wasn't intended to cover the type of liability that was at issue there.

And now, we're seeing, I think for the very first time, 2015 saw the first and most watched case, was a case that...a declaratory judgment action that Travelers brought for a coverage case involving one of its policyholders under a cyber liability policy. A district court in Utah decided that case and found there was no coverage in that particular instance, and it was kind of the first one out-of-the-box. So we're all still processing that case.

And another case was brought a little later, I think in June or July. Continental Casualty filed a declaratory judgment action in California seeking to disclaim coverage under its cyber liability coverage. And that case suffered a fairly quick fate when it was dismissed essentially for a procedural issue. In the policy, there was a provision requiring that the parties mediate before they file anything in court, and so that the judge summarily punted the case before ever analyzing any of the coverage issues.

So we haven't really seen much yet on the new policies, and it's tough to get a real gauge on the coverage issues that are going to arise in what is the second wave. But over the next 5, 10 years, these policies will be tested and we'll have a good sense of what they do and don't cover, and companies will be able to more informatively purchase the coverages they know they'll need for their particular liabilities.

Joe: And, John, as this second wave as you called it, moves forward and perhaps there's even a third wave down the line, from what you've seen thus far, and I realize there's not a huge track record yet, but are there some hot coverage issues that are emerging, and in particular, certain inclusions that may become hotly litigated in these cases going forward, even under these new policies that are actually designed for cybersecurity itself?

John: Well, I think one area that will be determinative of how these new policies cover these new risks will be in the definitions of terms that are used, particularly in the insuring agreement because as each claim, and every claim is unique. You never really know what you're going to get and how it's going to test your policy until the claim comes in. As an example, I'm looking at a case right now that was recently decided by the New York Appellate Court. And with some struggle, it came to the conclusion that what really amounted to a Medicare fraud scheme allegedly perpetrated by providers at a healthcare company, was not covered under a specialty add-on rider, cyber liability-type coverage rider, because it required the event to be any type of a hacking event that would be covered only if it was perpetrated by an unauthorized user of the system.

Well, in this case, the physicians were authorized users of the healthcare company's computer systems. So when they entered fraudulent Medicare claims for the purpose of getting reimbursement for services they didn't provide, the court said, "Well, there are some things that aren't necessarily clear about the policy, and some of the terms, it's very clear that it wasn't written for this purpose. It was written for the purpose of protecting against hacks by outside unauthorized users."

So there's an example of where you're going to find a term becomes very important that you wouldn't necessarily foresee, but we'll also see some of the standard issues that have been tested under various types of insurance policies in a new context. So things like late notice, which is a much litigated issue in the property casualty coverage world, did the policyholder quickly enough notify its...an insurer of a claim? Oftentimes insurers can be prejudiced if they don't learn of a claim quickly enough.

Well, that's going to be a hot issue with cybersecurity coverage because the response is so important, and it's so important that it's immediate. So notice is going to be key issue. Prior knowledge is an often litigated issue under any type of coverage. It's going to be a particular issue here because insurers are underwriting these new policies, and they're fairly scrutinizing what the policyholders' operations, their network security, and that type of thing.

But if the proposed policyholder is aware of certain liabilities that it has maybe already incurred or a claim or a letter that it got, that would indicate it's heading for a claim, did they have knowledge of that when they applied for the insurance might be an important issue.

Other insurance clauses, how do these policies interact with the other policies in a company's sort of regime of insurance? They have their CGL policy. Maybe they have a risk of fiduciary liability policy, and then they have a cyber liability policy. And depending on the nature of the claim, there may be some skirmishes between insurers trying to figure out which policy should be responsive.

So it's tough to predict, but I think we'll probably see some coverage litigation in those areas for sure.

Joe: You touched on something about a case where the issue was whether there was an unauthorized user who had perpetrated the event. And it would seem to me that it's an important factor here for insurance companies and their insureds to understand, and that is that these events, the triggers can vary by industry. And there are some data we've seen from Ace, for example, that shows that in the healthcare arena, the biggest problem, the cause of these events, is a rogue employee. Whereas for the retail sector, it might be a hack.

I would presume that there's some significance there for coverage issues just as there would be if it were determined that the cause of a data breach were perpetrated by a state actor or something that could implicate an act of war or terrorism exclusion. Do you have any thoughts on that, John?

John: Well, right. Different industries are...the energy industry for example, would have different triggers than you'd see in a health industry. Some industries...let's take Sony for an example, they're the lucky company that's had two very well-publicized acts of...or cybersecurity issues I guess we could say. The first, as we discussed earlier, was the PlayStation case, which was a fairly...what we would now call a typical data breach now that we've had the experience of seeing Target

and all these other companies, but Sony's was one of the first.

But more recently they were involved...their movie studio's operation, Sony Pictures, was involved in an issue with a nation-state actor. Allegedly North Korea attempted to shut down Sony Pictures from publishing their film that portrayed North Korea's president in a rather hysterical light, but they didn't care for it. They wanted to essentially extort Sony into not releasing the film, and the method of doing so was to reveal emails that Sony executives had sent to each other that were off-color and embarrassing for the people who sent them and really created reputational damage for those individuals and for the company as a whole.

So yes, different industries will see different triggers, and even within an industry, you may see multiple different types of triggers of these types of events. So we're keeping an eye on that. We obviously have our cybersecurity task force that you and I both sit on at our firm, and we have liaisons to our various industry groups that the firm represents, and different issues are going to come into play depending on the industry group.

But for insurers, all those industry groups are their clients as well because they're selling them insurance and having to deal with their claims. So in a big way, they're really driving the bus here. Loss control services, for example, are key insurers to even purchase the coverage. In some cases, insurers recommend or incentivize their policyholders to take better control of their cybersecurity measures. In some cases, it's required to even purchase the coverage that you submit to a certain protocols dictated by the insurer or maybe the broker.

I read an anecdote from Aon. The insurance broker was visiting a proposed insured to evaluate him for cyber coverage, found that 19% of their employees still use the default password assigned to them when they first began working there, which was P-A-S-S-W-O-R-D, which is not exactly high level encryption. And they that found an additional 23% had their new passwords on notes stuck to their computer. So prospective policyholders shouldn't be surprised that some additional costs beyond just the premiums of purchasing the coverage to include additional technology and protocols, like multi-stage authentication at the front end or insurers may require that they have a dedicated public relations firm, other response teams prepared to act in a case of a breach at the back end, just in order to secure the coverage in the first place.

So this is really a win-win situation for all involved. It's going to result in better cybersecurity, which is a boon for consumers whose sensitive data is at risk. It's going to reduce the costs to the policyholder. It's going to drive down premium costs ultimately, and insurers are going to be paying less in claims. So really, property casualty carriers are, in many ways, leading the charge.

Joe: John, you just talked about costs, and that's a nice segue to a discussion of the business of cyber insurance. We talked at the outset of this recording that the premiums by some estimates were $2 billion in 2014. Are these new policies expensive, and if so, why is that the case?

John: They're pretty expensive at this stage. They range, obviously depending on the size of the company and the amount of coverage, but anywhere from $7,000 or so for a smaller company, up to $50,000 or more for larger companies. And that is a direct function of the enormity of the claims experienced thus far. Their insurers have...generally they've paid out on the back end, so the coverage isn't cheap, but it can be expected probably that it will, in the next four, five years, we will see those premiums start to go down hopefully as more companies purchase cyber insurance and are looking more closely at their cybersecurity protocols and programs to make sure they're in top shape so that they can get their premiums reduced, and that, in turn, is going to mean there's going to be fewer claims. The claims that there are going to be less costly. They're going to be mitigated more quickly.

So we'll see the cost go down, but they're...it's always going to be a function of the claims experience, and right now, we're seeing very, very large claims experience, and it looks to be growing.

Joe: I found...I noted, one study of the average cost for a breached company total cost to $10 million over a 24-month period, and there's certainly a number of other studies with similar findings. These claims that you talk about being so significant, do they cover or do they encompass first and third-party losses or costs, and would you please explain what those terms are and how they are different?

John: Yeah, sure, and there are big components of both first and third-party losses at issue here. Generally, the cyber liability policies are just that, liability policies, which means they cover and are meant to cover third-party losses, but companies are now writing first-party coverage as well because there are additional costs beyond just the amounts that need to be paid to the parties that are allegedly injured by the data breach.

So a first-party loss is a loss made by the policyholder itself for some loss that it sustained. And in the case of cybersecurity, you would include PR costs, like I mentioned, notification costs to notify all the affected consumers, credit monitoring costs - that is pretty standard. Companies, when they suffer a data breach are required, typically by regulation or statute, to provide credit monitoring services for the consumers that are affected, and other things like reputational damage. Maybe extortion expenses, and just the actual loss of raw data, which is obviously critical to companies' operations.

So those are some of the first-party losses, and there are certainly coverages, cyber coverages designed to cover first-party loss as well. It's something that a prospective policyholder needs to keep in mind. And then third-party costs are costs that the policyholder has to pay to others as a result of its data breach. So that would include regulatory penalties, civil fines, legal expenses, paying for the lawyers who are defending the claim that inevitably comes and we've seen...I know you could talk for hours about class actions and derivative claims, shareholder derivative suits, and ultimately they're, at the end of the day, judgments in settlement dollars, that the policyholder is responsible for. So that's the third-party element. So if they do cover both and it's something for proposed insureds to keep in mind to make sure that they have coverage in place for all those elements of possible loss if that is something that they foresee for their particular operation.

Joe: And in covering those variety of costs, is that an example of why there's been this move to dedicated cyber insurance policies to supplement gaps that might otherwise exist in a company's other insurance policies, be it D&O, E&O, CGL? Is cyber insurance there to supplement all of that?

John: Yeah, and it's really meant as an all-encompassing coverage for any type of cyber loss. So for example, a company might have a crime policy, and it might cover a rogue employee sabotaging a computer system. A cyber policy would also cover that, but the crime policy wouldn't cover business interruption costs, for example, or identity theft monitoring expenses, that type of thing. It's really meant as a one-stop shop to cover all those potential cyber liability exposures that we've been talking about, restoring digital assets, forensic expenses, hiring forensic experts to investigate and determine what in fact happened.

And as I noted, regulatory fines and penalties, these types of things may or may not be, and are likely not covered under your typical property policy or professional liability or a kidnap and ransom policy, all of which may cover one particular sliver of the types of claims that could be made, but a cyber policy should respond really to any of those. So there are a lot of gaps that they cover, and it would, at this point, I think be beyond foolish, but potentially liability creating to not have this type of coverage in place. You can imagine a shareholder derivative suit. If the shareholders found out that there was no cyber liability coverage in place, for example, that might be a dereliction of duty and something not covered by the business judgment rule.

So cyber liability coverage is absolutely critical for any business really. There's no business that doesn't peddle in data, in electronic data. It's really now a critical component of any insurance regime.

Joe: And I think that's a good point to pivot towards some concluding remarks as we wrap up here, John. Given all of these issues, what are the themes that you are stressing with your insurance company clients looking out two, three, four, even five years down the line into this brave new world?

John: Well, I think with our health and life clients, as with clients in other industry groups, the theme is really regulatory compliance, making sure that their house is in order. The breach will come, we know that. So you need to make sure that you're doing everything you're supposed to be doing to try to prevent it and/or mitigate it when it happens. And that's an ever-changing landscape right now. There's so much action going on in the regulatory landscape for health and life insurer clients and property casualty insurer clients. A lot of that is coming from the state insurance departments, but as you know, there are numerous state and federal agencies involved in the regulatory picture.

And for our P&C clients, of course, we're stressing the same issues, regulatory compliance and whatnot because they too are subject to regulatory action and are themselves potential victims of cyber hacks and things. But also, more importantly, they're, again, like I said, the ones really driving the bus here. So coverage issues are big. We're now going to start testing these new policies. So the insurers really need to be careful with how they're writing these coverages and making sure that they're being very clear in the coverages that they're writing as to what exactly they are covering and what they are not covering.

So coverage is a big issue, and it's going to drive the claims experience in a lot of ways, too. We're going to...for example, when we saw Sony got the no coverage ruling, it really potentially affected the market, and I think that was a big event in

driving up the premiums for these new policies.

And I think looking down the road in five years, the scene will become a bit more normalized, according to predictions that I'm seeing currently. The market will still be expanding at that point but at a slower pace as the take-up rate of cyber coverage grows, hopefully closer to 100%. As I indicated earlier, I think that that means premium costs are going to go down. Claims will be fewer and less costly, and the coverage issues, under the new policies, will have evened out somewhat by then.

We're always going to see coverage issues just as we do under old policies with all types of different claims. But I would say in five years, we'll have a much better handle on exactly what these policies are going to cover and what they're not going to cover. So much turmoil now, and I see smoother waters ahead, and largely, again, driven by what these insurers are doing and experiencing out there on the front lines.

Joe: Well, that's great, John. Thank you very much for those observations and for walking us through this dynamic and really critical issue for the insurance companies that you counsel, and then as you noted, really any business out there that cannot ignore cyber insurance as an important piece of their overall firm's cybersecurity. So I'd like to thank you for your time and your valuable insights. And with that, wrap up this edition of *Carlton Fields on Cyber* . Thanks, again.

John: Thanks, Joe and Christina.