Lowenstein Sandler's Insurance Recovery Podcast: Don't Take No For An Answer

Episode 39
The Downstream Impact of Ransomware on Cyber Insurance Underwriting – Part 1

By Lynda A. Bennett, Robert DiRico and Shiraz Saeed
MAY 2022

Kevin Iredell: Welcome to the Lowenstein Sandler podcast series. I'm Kevin Iredell, Chief Marketing Officer at Lowenstein Sandler. Before we begin, please take a moment to subscribe to our podcast series at lowenstein.com/podcasts. Or find us on iTunes, Spotify, Pandora, Google podcast, and SoundCloud. Now let's take a listen.

Lynda Bennett: Welcome to "Don't Take No For an Answer." I'm your host, Lynda Bennett, chair of the Insurance Recovery practice here at Lowenstein Sandler. Today, I'm very pleased to be joined by two guests: Rob DiRico, who is the Cyber Liability National Practice Leader for ARC Excess Insurance, and Shiraz Saeed, Vice President and Cyber Product Leader for Arch Insurance. Thank you both for joining us today.

So, today we're going to be talking about what is probably the most hot topic in the entire insurance industry; it's cyber insurance coverage and particularly, we want to do a deep dive into what's going on in the underwriting of these policies. Many of my clients ask, "Is this market going to continue to exist? Are insurers going to continue to be willing to issue policies to cover these types of risks that seem to be rampant?" The claims activities are through the roof and there are no two better people I can think of to bring on than Shiraz and Rob, because you're living and breathing this every day. So let's jump in with a high level question. What's the current state of the market in terms of capacity, premium, self-insured retentions, and terms?

Rob DiRico: Shiraz, if you'd like, I'll start up and then you can chime in. Right now, this market is the hardest it's ever been. I would say last year it started to really shift significantly and at that time you were looking at premium increases overall on insurance programs in the 30-40% range with retention shifts and coverage restrictions, such as supplements on ransomware related events and co-insurances, which was typically subject to underwriting criteria. If there were certain protocols not in place, an insurance company would apply those types of restrictions.

However, what we've seen as drastic then, pales in comparison to what we're experiencing now. It's not uncommon to have insurance programs increase a hundred percent to 200% or 300% in some cases with massive retention shifts. In terms of insurance underwriting capacity, the days of the $10 million limits have been severely limited. You're seeing insurance companies cut their limits from $10 million to $5 million on a very common ordinary basis. You can still get $10 million in capacity, but it has to be with only a handful of

insurers that feel very comfortable with the placement, have been on the risk for a long period of time, and have not suffered maybe as significantly as other large household name insurers, where you'd be shocked that their approach in that they are cutting capacity.

Lynda Bennett: Yeah. Shiraz, what are driving the claims and leading insurers to think a little more carefully about their underwriting process?

Shiraz Saeed: I agree with a lot of things, Robert was saying. I think the first thing that we need to sort of level set here is most carriers are breaking these companies into three major buckets: small or SME, midsize, and large businesses. And the approach that they take towards each marketplace is sort of how they are determining the rate structure in those things. When we are looking at a risk, the downstream impact of a ransomware impacts multiple insuring agreements of a cyber policy, and depending on the size of the company, the impact of the ransomware will determine the downstream loss: whether you're going to lose $150,000 on average versus $2 million on average versus five or $10 million on average. So each company is looking at their losses and seeing where that average is, and then trying to create a rate structure or premium structure that allows them to stay profitable within that range.

So think about if we wrote a policy for a $5 million limit and in year one, we suffer a ransomware incident and the whole limit is paid out, the whole $5 million. How much money would we have needed to collect in year one, plus how many years would we need to make our money back? An average loss run shows five years losses. So if we use that as the payback period, because that's the only time somebody's actually going to know about it, if we had that $5 million loss, I would need to charge how much to make that back?

So let's say hypothetically, you had a $100,000 SIR. So now that means the total insurable loss is actually $4.9 million plus whatever premium you had collected in year one. Hypothetically speaking, let's say that was $100,000 also. So your net loss is $4.8 million. Well, how much would we need to charge to get $4.8 million back in five years? A million dollars a year. That means our premium needs to be a million dollars. “Whoa Shiraz, that's like $200,000 per million dollars that you're putting up. That's a lot more than the $20,000 you were originally charging me.” So now, if we take that understanding and your average loss is $5 million on a ransom,, well, your rate's going to need to come up to 200K per million in order for you to be sustainable.

So each carrier has their own loss ratio and has to think about the payback period and has to think about how much premium they would need if they suffer the loss in year one versus year two and so on and so forth. And based on that, you're going to see rates developed. In addition to that, what I would also say are very important drivers and I think we'll talk a little bit about later also is how do we categorize the class of business? And I could tell the audience there's three major buckets that you could be in.

One is a business to business with no consumer private information. You don't deal with the general public. That would be a construction company, an A&E design firm, would be examples of this. Transportation and logistics. Then there would be group two, which is direct to consumer. That's companies that deal with the public: hospitals, schools, retailers, that type of stuff. And then the third bucket is a business to business that exchanges customers' private information on the computer system. So all of these companies are suffering ransomware and business email compromises. It's just that downstream loss is less for group one because they'll have to investigate, negotiate, recover their data, lose the income; but they're not notifying, identity monitoring, having regulatory proceedings. Group two would have that.

And in group three, you have all of that plus an errors and omissions issue because it's their professional service to protect the information of the computer system. So depending on how much the carrier's losing and how much they need to get it back, plus the class of business and the revenue size and employee count, these are the factors that are going to drive the rate. But there's one more thing: The controls. There's a renewed emphasis in the marketplace about controls and that is a big driver in all of this.

Lynda Bennett: Yeah Shiraz, I was going to comment that from the policyholder's perspective, there's a lot of tension right now in where they're putting their dollars. So it's putting it into premium dollars, it's taking on greater self-insured retentions, meaning your dollars first before you're going to get to real insurance. And I'm glad that you brought up the notion of controls because obviously putting more money into better security and more knowledge and attention and resources around, knowing what your records are, where they're kept, better training for your employees who are probably the weakest link in a lot of the losses that are happening right now. It really does require policy holders to think very broadly about their approach to risk management and buying an insurance policy is one piece of it, but really becoming a better risk is another piece of it. So I'm going to go a little off script here and ask both of you, how much are policy holders making use of the loss prevention services that insurers are offering and, if they're not using them, why do you think that is?

Shiraz Saeed: So just to give some background, I've been trying to offer loss prevention services with the cyber policy for many, many, many years. And in the beginning there was, I would say between 2012 to 2018, a proliferation of cyber insurance; where if you were below 250 million in revenue, the frequency of claims was so low and the margin of profitability was so high that every carrier basically wanted to get into the space. And since it was so competitive for pricing, some smarter carriers came up with the idea that we should offer services along with this, to round out the program and also to help customers that are deficient in controls.

That was sort of the logic behind it. Well, now a lot of those services or offerings that we were trying to give to them are must haves to just get a quote. So it's not like, Hey, let's get you some detection and response EDR services, where we get you for a discount or something; it's like now, no, you can't get a quote unless you have it on a hundred percent of the network and you have it with a reputable company. Another example would be training.

That's something that a lot of carriers offer, through either a law firm or cybersecurity firm. Well, if you're not doing training in cybersecurity, at least once or twice a year, you're not going to get a quote.

Lynda Bennett: So Rob, are you seeing with your client base that where there was a resistance, now maybe less so, or is there still a high level of skepticism in using those loss prevention services?

Rob DiRico: So I can say right now, I think that the selection of risk management services is completely personality driven. In my opinion, I would say if we just want to get into numbers, a third of my clients like to pursue all risk management benefits or that or services that the insurance company can provide. You can have very savvy risk managers or larger companies love to be proactive and take advantage of it and want to adhere to all the guidelines that the insurance company can provide them and put in place a lot of them, put those value added benefits to practice. But I can also say that you do get an adversarial approach too sometimes. I have many clients that the IT feels like they are the best in business. They don't understand why the insurance company's asking these questions and it kind of proves sometimes, and I hate to say, a little bit of their arrogance or ignorance in that, the insurance companies have seen these losses and that's why they're calling in on certain things.

You will get the occasional person that hears something and has a blurb about it but I also think education from the broker standpoint is even more crucial. Many of our clients, a third want to be involved, the other third doesn't know because the broker might be selling them, the insurance policy, not telling them that, oh well, when you purchase coverage with Shove, you can get these types of reports or penetration testing for a much lesser charge. If you're with Beazley and you're a certain type of policy holder, they can do a whole scenario for a breach to see how your company responds. Like Shiraz said, they will give you efficient training for all your employees with a certain partner or a vendor at a great rate.

So it's really a blended approach, but I can say those clients that pick the risk management and are on board with the carrier and do pre-screening for how to handle a breach and how the carrier works with the breach itself and puts in place all the value -added services they have, the more they're loyal to the insurance companies, the better. They're much more loyal because they see the benefits added and it helps explain the market to the insureds. And obviously most importantly, they're better protected as a business.

Lynda Bennett: Yeah, and really leveraging the insurance. I know from my experience with clients, the insurance industry right now is putting in a lot of resources themselves. They maintain a lot of information and really leverage the relationships that the carriers are building with them. Some of these specialists are a real value add. I'll just add two with policy holders, Rob, you touched on it. There's a high level of suspicion and everybody thinks all of their information is highly confidential and it should be like Fort Knox and letting any stranger in is just a no-no from their chief information folks.

Rob DiRico: There's also risk management from the insurance companies that continues while the policy is enforced. So now what you're seeing is a lot of insurance companies will send a notice to the policyholder and CC the broker stating we've just been on our scans, we've tracked these three vulnerabilities and we'd like to see what you can do to remediate, and we can have a call to fix them or take next steps. That has gone either positively where the client sees them, is appreciative, and fixes them. Or the client will literally say, I don't trust this email. I don't know who this person is, which actually shows that they're risk averse. And there have also been cases sometimes where the insurance company might have got it wrong, where their report wasn't up to date, and it was already fixed. But I just wanted to point that out with your comment.

Lynda Bennett: No, I appreciate that. All right. So are there particular industries right now that are very difficult to ensure?

Rob DiRico: Yeah, I would say in my experience insurance companies run for the hills when they see a municipality or government entity- the controls are so below what industry standard is. And hospitals are a higher hazard class because they have that class of business that Shiraz mentioned where you're dealing with customers, but they're also having regulatory issues with the personal information. So a full scale breach can be much more costly. That class of business is automatically declined by many insurers, even if they have pristine protocols. So those are two industries where I find vendors. And of course Shiraz can elaborate on some other classes business.

Shiraz Saeed: Sure. Besides the funding issue for controls, which some might argue that the federal government has provided some extra funding for over the past couple of years through some legislation, the real concern right now with public entities is also state sponsored. And if it's a state sponsored attack against a town, a city, those types of things. So that's another, what I would say, gray area for a lot of carriers. So just I wanted to point that out, besides that, I think one of the most dangerous groups right now is managed services providers. And that falls in that third bucket, I was mentioning earlier, where they're in the business of exchanging people's private information and/or managing or hosting the computer system.

Those companies are the most dangerous and one of the highest hazards because they have an aggregated exposure in addition to their individual company. Multiple companies will be impacted based off of their one incident. This is not something new in the industry. So that aggregated exposure is what makes them sort of dangerous and tough to write.

The other group that I would say is still very difficult to write is FinTech, because the digital economy and ecosystem is not completely regulated. So a perfect example would be a crypto digital wallet. Is that a bank account? Is it FDIC insured? What happens if the money is stolen from there? So that regulatory concern; and then the second thing is the tech: is it a financial service or is it not?

Technology errors and omissions is software code was programmed wrong, thing didn't work right, we lost money. When I say software code didn't work

right, now I violated a federal regulation for a financial institution. Now wait a minute, is my covering for technology errors and omissions, or am I covering financial services, and E&O? So that becomes a challenge as well. So a lot of the stuff that's traditional financial services, most technology errors and omissions and cyber carriers don't want to cover that. There are definitely a couple of markets that see this and they'll have like a package policy where it gives it all, but it's definitely something tough to write.

Lynda Bennett: And that's why you need an excellent broker like Rob. So we've just barely scratched the surface of what is a very complicated and hot insurance area. So I'd love to have you come on back to continue the conversation in another episode, if you'd be available to do that.

Rob DiRico: Happy to do it.

Lynda Bennett: All right. Terrific. Thanks. And we'll have you back real soon.

Rob DiRico: Thank you.

Kevin Iredell: Thank you for listening to today's episode. Please subscribe to our podcast series at lowenstein.com/podcasts, or find us on iTunes, Spotify, Pandora, Google podcasts, and SoundCloud. Lowenstein Sandler podcast series is presented by Lowenstein Sandler and cannot be copied or rebroadcast without consent. The information provided is intended for a general audience. It is not legal advice or a substitute for the advice of counsel. Prior results do not guarantee a similar outcome. The content reflects the personal views and opinions of the participants. No attorney client relationship is being created by this podcast and all rights are reserved.