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

Episode 15 -
Cyber Insurance Coverage Market:
A House of Cards or Temporary Plateau?

By Lynda A. Bennett
Guests: David Finz and Steve Shappell

MAY 2021

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," an Insurance Recovery podcast. I'm your host, Lynda Bennett, Chair of Lowenstein Sandler's Insurance Recovery Group. And in today's episode we're going to be talking about the cyber insurance coverage market. Is it a house of cards or are we just hitting a temporary plateau? With a couple of quarters of 2021 nearly in the books, companies continue to see an alarming number of security breaches and ransomware attacks. Each time we prepare our workforce for how to combat the latest cybersecurity threat, the bad actors seem to be two steps ahead with their next scam. A few years back, we were all learning about social engineering and how to make sure that an email from our CEO really came from her and not an imposter. So now, we are all carefully scrutinizing the emails in our inbox while hackers have moved on to manipulating invoices and payment instructions for our customers and vendors.

At the same time, we continue to see ransomware attacks across every industry. The price of ransoms have skyrocketed from five to six to now seven figures. Regulators remain active in the space, imposing significant and differing standards in terms of maintaining personal information and notifying persons impacted by a breach. Now, fortunately, most companies have dedicated cyber insurance policies in place to help navigate them through many of the adverse consequences that flow from a security breach. However, the question that's on my mind today is, how much longer can this last? Will the insurance industry continue to write these policies and pay claims without a fight? In order to probe these important issues, I'm fortunate to have with me today, David Finz, Vice President of Cyber Risk at Alliant Insurance Services and Steve Shappell, Alliant's Specialty Claims and Practice Group Leader. Welcome, David and Steve. Pleased to have you here today. So let's start at the high level. Is the cyber insurance market sustainable? Or is it a house of cards that's going to fall under the weight of the relentless claims activity that we've seen over the last year or two?

David Finz: Well, first of all, let me start by saying thank you for having us here today. My response to that is I think what we're seeing is the growing pains of a still relatively new line of coverage. This is not a house of cards. What we have seen is that the market is going to need to become more sophisticated in the underwriting process. Over the past decade, decade and a half, as we've watched the cyber insurance marketplace develop, there's been an abundance of capacity. The underwriters were generally relying on paper applications and brief phone calls with an organization's CISO or CTO in order to get a sense of the security controls. That's no longer going to suffice.

Now, they're beginning to incorporate security scans and other types of non-invasive testing of security controls as part of the underwriting process. This is forcing both organizations and their brokers to up their game and to help clients differentiate themselves and present themselves to the markets as a better risk. In fact, the underwriting process itself is an opportunity for organizations to conduct a risk assessment and thereby strengthen those privacy practices and security controls. So we see this as a positive development. We're embracing it and we understand that it is a hardening market, but we are helping our clients navigate it.

Steve Shappell: I would agree with that, David. The other observation, following the claims carefully and comparing and contrasting this to other products that have developed over the last couple of decades. The underwriters here are, they're paying attention. They're doing a nice job of thinking through attachment points of what's the proper retention? What's the proper limits of liability to put out there? A lot like we saw with other products like [inaudible 00:04:39] employment practice, is a pretty good example, where attachment points were too low and capacity was too high. Underwriters thought it through and, I think, did a nice job of figuring out what is a proper retention, what is a proper attachment point, what is a proper limit of liability to put out there.

Lynda Bennett: Steve, are you saying that we're going to see a series of sublimits put on these policies in the different coverages that are there? Or are we going to see the scale back and the right sizing of the market in a different way?

Steve Shappell: David and I will probably debate this. I think we'll see carriers attempt to do sub-limits. That way they can continue to collect premium for larger limits of liability, but then sublimit it and reduce the risk. I think we, the brokers, are going to continue to push very, very hard that sub-limits are not good. They're the devil. Nothing good comes of a sublimit. So we'll have some really interesting friction in the marketplace, which is healthy and normal.

Lynda Bennett: David, I think there was some bait thrown in the water. Are you going to take it?

David Finz: Yeah. There's really not much daylight between my position and Steve's on that. Obviously, from a broker standpoint, we want to try to get full limits for our clients across all the insuring agreements of the cyber. We understand that the ransomware epidemic, for lack of a better word, that has fallen upon businesses has had an impact on loss ratios for the underwriters and that they are scrutinizing that more carefully. But again, I think the solution to that,

ultimately, is to have organizations reevaluate their security controls, their employee training practices and present themselves as a better risk to the markets. We believe that through that process of differentiating them, that we can still achieve favorable coverage terms for our clients.

Lynda Bennett: Does that mean that there are going to be winners and losers? If the insurance industry is going to scale back, are there particular industries that should be concerned that it's going to be harder for them to either secure coverage at all, or to secure the same levels of limits that they have in place today?

David Finz: I'm not sure that it's going to be specific to industry. Again, up until a few years ago, certain industries were more likely to purchase cyber insurance than others, basically, if they had large quantities of consumer data. So healthcare organizations, financial institutions, retailers, they were the early adapters along with any type of e-commerce companies. Over time though, as more of an organization's operations go online, whether it's inventory, payroll, now we have a situation where, as many organizations have become paperless, whether it's in the finance, insurance, real estate sector, whether it's in manufacturing, we're now at a point that the need for cyber insurance is across all industries.

As far as market segment size, there is still large, untapped growth potential among small and medium sized businesses, many of whom still do not purchase the coverage and are evaluating it for the first time. So I think more than based on industry or market segment, the differentiation is really going to be around who takes cyber hygiene seriously. That is something that as their risk consultant, as their insurance broker, we can help connect them with vendors that can improve their security posture.

Steve Shappell: David, do you anticipate that we will almost go backward in some of the underwriting? Because when I think back to cyber underwriting in early years, it was really, really cumbersome. They spent a lot of time on our client's business. And then it got lax. Do you think we're going to go back to, not necessarily the old ways, but the old days where they're just going to be a lot more invasive with understanding how our clients do business?

David Finz: I think there's definitely going to be more scrutiny as part of the underwriting process, but I don't know that it's going to be as cumbersome as it was five, ten, fifteen years ago. Clearly around say, ransomware, now there are supplemental questionnaires that many of the carriers are asking for as part of the renewal process. I joked recently to one of our colleagues, when I looked at one of the carrier forms, I said, "I would look at this and say, 'They're trying to play 20 questions with our clients, but there's actually 30 on the form.'" So it can be cumbersome.

David Finz: But the difference between now and in the earlier days of the cyber insurance market is the availability of these tools that can come in and do the IT security scans and give the insurer an understanding of the security controls in place, not only in terms of the network itself, but what kind of information is available on the dark web with respect to an organization. These are analytical tools that have been adapted by many of the insurers. We,

ourselves, as brokers, have access to similar tools as well to help our clients prepare for the renewal process and identify any areas where they do have vulnerability.

Lynda Bennett: That's a tough nut though, David, to sell to clients, because they are extremely reluctant to let anybody, let alone insurance companies who haven't paid a claim yet, come tramping through their system to know where all of their super-secret documents are, to give them essentially the keys to the electronic kingdom. I think there's going to be a lot of education that's going to be required to get the policy holders comfortable in seeing the benefit and value in doing that type of sharing, especially on the front end and placement phase.

David Finz: Well, the security scans we're talking about are noninvasive in nature and in fact, can be conducted without having access to a company's network. So we're talking about the cyber equivalent of a drive by to see whether there are any broken windows or newspapers piling up in a stack on the front stoop. These are indicia of vulnerability that are evident to cyber criminals without having to go into a network. Therefore, these are things that an organization would want to know, irrespective of whether they're purchasing cyber insurance, so that they could address these virtual broken windows, so to speak and shore up their security. This does not require invasive penetration testing or anything to an organization's network. Again, these are tools that are available to both the ethical hacker, as well as to the cyber criminal element.

Lynda Bennett: Well, so before we move on to the next topic, though, I do want to press you, David and Steve, a little bit, what is the incentive for the carriers to continue paying these ransomware demands? How much higher can this go? We started out with average figures at five-figure settlements. We went through six pretty quickly. Now we're seeing seven figures. It seems natural that the next trend is going to be eight-figure demands. How much longer can this continue, where the carriers are going to be willing to pay those claims quickly and seamlessly?

David Finz: Well, I think one of the things that we need to keep in mind in response to your question is that payment of the ransom is actually a last resort on the part of the carriers. When a threat consultant is engaged, there are several steps in the process that are taken to try to relieve the burden of having the insured make the ransom payment. That's one of the valuable services that cyber insurance provides. The first step is a threat consultant comes in and tries to ascertain whether the threat is credible. Do these threat actors actually have access to the network? Are they bluffing? Do they have the data?

Secondly, what do we know about their M.O.? Do they seem like the types that will actually make good on their threat? Do they have a track record of once receiving payment, calling off the threat? Another service that is available is that many of the threat consultants actually profess to have the capability of reverse engineering the IP address so that they can identify whether these threat actors are in any way associated with a sanctioned individual or entity, because we're all mindful of the fact that the Department

of Treasury is watching very carefully to make sure that payments are being made to sanctioned parties.

So all of these steps... Oh, and I overlooked one. Does the FBI or some other law enforcement agency have the decryption key for this particular threat, such that the ransom payment does not need to be made and that the insured can get out of this mess without having to resort to making the payment? So all of these steps in the process are taken to limit the frequency with which ransom payments are made. Again, it's not for me to do the carrier's bidding, but I believe they would agree that to the extent that they make payments, they do so as a last resort.

Lynda Bennett: Great. All right. Well, Steve, let me throw this one over to you, because again, as we've been talking about the premiums in this space are going up exponentially due to the claims activity. And many of our clients are trying to fill out their shopping list and trying to figure out where best to deploy their financial assets here. Are they better off to continue buying this coverage as it continues to get a bit more expensive? Or are they better off just layering on additional security measures to keep the enemies at the gates?

Steve Shappell: So the answer is yes. It's both, as you probably would expect, because companies are spending a great deal of resource and focus on security. Despite that we have event, after event, after event. I don't know how generally a company's going to sleep comfortably at night, picking one over the other. You can't just buy a lot more insurance and then just give up on your efforts internally on security. And you certainly can't do the opposite, because as we've seen, unfortunately, and sadly, the bad actors are actually pretty good at being bad actors. They're going to continue to find ways. I think the focus has got to continue to be on both of these. As this product gets more expensive, as they have and they endure more and more losses, we'll have to figure that out.

That's why David makes the big money, is he'll solve for this in the policy placement and the attachment points and the retentions. We'll solve for it so that the market remains viable. So that's my view, is the answer is both.

Lynda Bennett: All right, well, you've both convinced me that this is not a house-of-cards market that's going to fall into itself. So let me just ask you to do this. Polish up your crystal ball and let me know, where do you think the cyber market is going to be five years from today? What does it look like?

David Finz: I guess I'll start. I'm waiting for that big money. Maybe that'll come through in the next five years. Aside from that, I think one of the things that the market was going to have to solve for is the ability to deal with the question of the internet of things. As we begin to see more interconnected devices, the exclusions for bodily injury and property damage, which are already to some extent, getting chipped away at for computer hardware replacement costs, commonly known as bricking, and some other areas around the fringes, are going to need to fall by the wayside. Because what happens when medical diagnostic equipment or power grids or other, even self-driving automobiles, begin to result in claims where there is bodily injury and property damage? So I think that the market is going to need to address how that wall, which is

already semipermeable, is going to hold up in light of those losses in order for the coverage to stay relevant.

Lynda Bennett: I agree. I've had my Roomba chasing me and I'm waiting for that broken ankle, so we'll have to wait and see on that. So Steve, give me your crystal ball prediction on the claim side.

Steve Shappell: I think claims will continue to come in, and consistent with what David's talking about, this coverage is going to evolve. I think we're going to continue to see friction points, that the points going to get, on this spear, is going to get sharpened and sharpen and sharpened as carriers try to, I think, be a little more precise in their deployment of capital. We're going to continue to be aggressive to make sure that the evolution of these risks are covered by these products. I think it's going to be a very robust claims environment. I think it's going to be a very robust coverage environment, that on these large claims, when they come in, as the exposure to evolve and they get more and more interesting and unique.

Lynda Bennett: Well, I really appreciate that. And really do appreciate both David and Steve joining us today and sharing their knowledge and experience. One thing's for certain. This is certainly not going to be our last podcast episode on the cyber insurance market, because David has convinced me it's here to stay. So please do join us again next time. And thanks very much for your time today. Really appreciate it.

David Finz: Thanks.

Steve Shappell: Thank you, Lynda.

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.