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

Episode 8 - The Ransomware Attack Part 1 – How To Keep The Enemy At The Gates

By Lynda A. Bennett
Guests: Bridget Choi and David Anderson

MARCH 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, and I'm very thrilled today to have two esteemed guests with me, David Anderson and Bridget Choi. In today's episode, we're going to be talking about the current state of play in the cyber insurance market with a specific eye toward ransomware claims. In 2020 alone, there were more than 20 reported ransomware attacks in the US that impacted a wide array of industries, including government, healthcare provider and vendors, educational institutions, and many other organizations and industries.

The havoc that these attacks create is multifaceted. From the initial eye-poppingly large ransom demand, to the need for an immediate shutdown of electronic systems that are the lifeblood of companies today, to assembling a team of qualified and highly skilled specialists on the fly to come in and recon what happened, the how and the why did the intruders get in, to notifying impacted customers, employees, vendors, and other stakeholders, if information has been exfiltrated and what your company plans to do about that. To responding to the swarm of regulators who need to know what happened, why, and what the company plans to do about it? To the class action lawyers who are actively signing up new clients every day to pursue legal relief for damages that allegedly resulted from the breach. Add to the laundry list of these challenges that the bad actors typically and intentionally tend to unleash these attacks late Friday afternoons, so that the chaos that ensues becomes all the more difficult to deal with.

It doesn't sound challenging enough? Well, the reports from a number of organizations that closely monitor ransomware attacks have indicated that in Q3 of 2020 alone, there were more than 50% increase in ransomware attacks, and the price of ransom demands is skyrocketing. So what's your company to do? In the first instance, you should try to avoid getting hit. And in the second instance, be in the best position to nimbly respond if the bad actors make their way onto your systems. So for today's episode, we are fortunate to have two specialists, Bridget Choi, deputy counsel and managing director of strategy for Kivu Consulting, and Dave Anderson, vice president within Lockton Insurance, Cyber Technology Group. And they've both been working on the frontline of ransomware attacks on a daily basis, so they've got some great practical tips for us on how to avoid ransomware attacks, and how best to respond to them if Armageddon unfortunately does hit. So Bridget, why don't you take a few minutes to give us some of your experiences and background in responding to cyber threats?

Bridget Choi: So, I am a deputy general counsel here at Kivu, and I started my career like a lot of people as an attorney here in New York City, and then I moved to claims. And in my career in claims and insurance company, I was handling a lot of cyber claims. I did that for a while and helped a lot of insureds out of situations, much like ransomware, and I pivoted. I joined Kiva, which is an incident response company. And we are the companies who provide the immediate assistance, the investigation, and the recovery to victims of ransomware.

Lynda Bennett: That's great. And Dave, why don't you give us a few minutes about your background and experience, and how you help companies after that horrible phone call comes in at five o'clock on a Friday night?

David Anderson: Sure thing, Lynda and Bridget, it's so good to be with you both. As you mentioned, my name is David Anderson, vice president, and head of major accounts for Lockton Cyber Technology Practice here in New York. I guess you could say fundamentally I'm an insurance broker, but that role has gotten more complicated over time. We support our clients in identifying their exposures around cyber risk, whether that's privacy related, physical damage related, or products related. We help assemble a program with underwriters that effectively and deliberately addresses that risk with some risk transfer mechanism, usually insurance, because we are insurance brokers first and foremost. And then we are always at our client's side, even with the 5:00 PM, Friday ransomware call. So I work directly with our insurers to facilitate introductions to law firms like Lowenstein and vendors like Kivu to help put out the fire, rebuild the house, and get folks back up and running. So I've been there every step of the process, and I'm happy to be here with you both today.

Lynda Bennett: Well, I'm very pleased that both of you took time out of your day. And as is our style here at, Don't Take No for an Answer, we're going to keep our discussion very practical and in plain terms. And we insurance geeks are going to do our very best to give some great actionable advice today. So Bridgette, tell me what's going on? Why are so many companies getting hit with ransomware attacks these days?

Bridget Choi: Ransomware has been around for a long time, but it really picked up speed about four, five years ago. And what has happened since is it's a very vibrant economy now, they've made a lot of money. And these attackers have now invested in themselves. And what we see from the evidence that we pull together from the dark web, from forensic analysis, is that they operate like organized crime. There's a structure, there's a hierarchy, they can scale. So if they hit a very large company, they can outsource some of the negotiations for example, or they can bring in specialists to do something tricky in a tricky environment. And they have become much like any corporation and are truly now organized crime, much like any mafia family you would imagine. And that's really what has changed.

Lynda Bennett: So Bridge, what can they do? What can companies do to keep those bad actors at the gate and not getting inside?

Bridget Choi: The advice I typically give is there's really no silver bullet, right? And I know that's not comforting, but there are some basic things you can do to mitigate the risk. One would be preparation in accept that this is a risk that has proliferated and hit the highest companies and the lowest. So be prepared for that to happen. Have insurance, have a plan, practice that plan. And then on the preventative measure side, I would strongly recommend understanding the common vectors of the attack. They typically all get in through unpatched vulnerabilities in your gateway to the company, remote desktop protocol is another, if that is open through the internet, they can scan it, they can find it, they'll crack your password and get entry, and phishing emails. Those are the three ways they typically get in. So if you have a gateway vulnerability, if you have an open RDP, look to see that you are mitigating that. And then as always have MFA, make sure you have endpoint monitoring detection, and be vigilant.

Lynda Bennett: That's great. So, Dave, are there any resources available in the insurance space? You talked about insurance products, but before we get into the details of what it provides, what are the underwriters looking for in terms of risk management, risk prevention, at the front end of the buying process for a dedicated cyber policy to protect these types of risks?

David Anderson: That's a great question, Lynda. I think the biggest challenge that we're seeing and this alluded to what Bridget mentioned, is that the bar is getting higher every single day now in order for a specific company to be considered "insurable" for cyber risk, because of the severe uptick in ransomware claims specifically, insurers are looking for three specific threat factors to be really addressed exceptionally well in order for you to be an insurable risk. Bridget touched on two out of three of them. Multi-factor authentication for external facing connections is a must, multifactor authentication for privileged accounts, domain controllers, et cetera, is a must. Having some sort of non-signature based endpoint protection in place like a Sentinel one, which is behavior based is also a must because a lot of these ransomware strains slip right past the net of a signature based solution.

And then lastly insurers are going to actually make you represent and warrant, and in plain English that means promise to your insurer that you have effective, tested and resilient backups in place. Whether that's through air gapping, or in other words, separation from the operations or the network, or immutable backups, which is a fancy way of saying read only backups that can't be corrupted. Basically your underwriters are going to ask for you to demonstrate to them that you have a plan to get back up and running, that will avoid having to pay the ransom altogether.

These three data points were not a big deal six or 12 months ago, I think underwriters were still grappling with how to even properly underwrite the risk and know what pain points to look at. As of today, there are threshold issues. If you can't answer the question around all three of those data points affirmatively, you're either not going to be able to get coverage, or your cyber coverage is not going to cover ransomware related events. Lynda, I know answered your question on the pre-underwriting perspective. Do you want us to dive into what you can leverage your policies for as well?

Lynda Bennett: Yeah. I wanted to get into that. I have two questions really related to that. One is, a number of our clients are concerned going into the underwriting process with the carriers because some of the questions are quite detailed around what security measures are in place, and a lot of the IT folks of our clients aren't super excited about letting underwriters or insurers tramp through what they have in place, there's a lot of intellectual property trade secret information that's housed on the system.

So first question there is how do you manage around those issues of giving the carriers the confidence and assurance that they need to know that you're a good risk to underwrite while balancing not wanting to have to let the insurers tramp through your system to even get that policy in place? And then the second question, and you can take them whichever order you want, Dave. The second question relates to how policy holders and insurers can work cooperatively together in some of these pre-breach value add services that can be provided to help the policy holders really kick the tires on how good their security systems are already in place, and if there are improvements that can be put in place before the breach happens?

David Anderson: I'll do it in the order in which you asked, counselor, I think they're both really tough questions and the answers are, for those of you who don't know who I am, we don't BS, so the answers are going to be take them or leave them. Depending on who your insurer is, depending on what type of insurance structure you're looking to put in place, your insurer may be asking questions that are a little bit personal, for lack of a better word, right? Or intrusive around your controls. A lot of our clients either engage insurers with the support of an NDA in place. Some of our more sophisticated clients will engage counsel, shameless plug, Lynda, to negotiate with a broker on their behalf. I have never had a situation where representations made to the insurer, or the ability to have the insurer go in and snoop around or tramp through the system, as you mentioned, Lynda.

I've never had that be a situation where the underlying underwriting data was compromised in some sort of claim or discovery. So my response to a client that has that question, and Lynda, to your point, it's a very common question, is you're asking a third party insurance company to commit five or $10 million of capital, maybe 15 or 20, right? They have a right to ask questions, and with the claims frequency and severity that we're seeing in the cyberspace, I don't think that's going away anytime soon. You can probably get away without having to let the insurer actually come in contact with the network, hire some third-party vendor to provide an assessment of the network. But if you're comfortable and you can get your head around the confidentiality and contractual protections that you can leverage to ensure that confidentiality, you might actually be able to negotiate a better bargain by letting the insurer in on a more detailed level.

What I would also say is, five years ago, seven years ago, there was a lot of hesitancy from the CSO side of an enterprise to give the insurers a lot of information, right? And we used to get away with a lot less information when the market was different back in the day. We have seen a sea change now, culturally, where an organization, frankly, that is uncomfortable having a transparent and open dialogue with their potential insurers actually comes across as a worse risk than someone who probably may not have the best controls, but is upfront about it, has a frank discussion with the insurer, and then leverages the insurer's toolkit to make themselves a better risk, which answers the second question you made, but I'll stop there, Lynda, to see if you want to follow up.

Lynda Bennett: Yeah, well, actually I was going to throw it over to Bridget to talk about some of the services that Kivu may do before you've got a breach that, as I mentioned before, that kick the tires, bring somebody in from the outside. What types of things are Kivu doing for companies that will help enhance a policy holder's risk profile when they come to Dave to get their cyber policy placed?

Bridget Choi: One of the biggest risks out there is the risk we're discussing, ransomware. So, someone like Kivu could come in and do a vulnerability assessment that's specific to ransomware. We would look at your network and say, "Oh wow, we're looking at your assets, and it looks like you don't have enough controls around this, you don't have MFA on these crucial things. Wow. It looks like your backup is not offline and here's what could happen. Here's how these attacks move within your system. This is what the bad guys do." And it's instructive, it's eye opening, and it helps the company prepare, but it also helps when they correct. Some of the stuff is very simple corrections. When they make these corrections, it makes them a better risk. They can get more capacity, perhaps a lower rate. So that's what we do. We can provide other augment their security if they need it. But I think those are the things that really help David advocate for you with the carries.

David Anderson: To bolster Bridget's point, that was your second question to me. A lot of what Bridget just spoke about is actually available to policy holders from many of the insurers, right? Most of the market leading insurers in the space provide either a risk reduction budget which functions as a percentage of premium, or will offer complimentary or highly subsidized services to make you a better risk. So it's important that our audience knows that, right? Even if you may not have the budget or appetite to spend that money, your policy that you're already paying for probably has some sort of risk reduction credits built in. It's just a matter of asking your broker or trying to get an understanding. Anecdotally, the uptake rate on that stuff has been 3% and there's a lot of money that's just being left on the table and we try to get everyone aware of that.

Lynda Bennett: Yeah, that's a great point, Dave, and I did want to make the point because I get asked by clients a lot. "Well, I don't want to use the insurance company's chosen vendors because they only choose the cheapest, not the best." And that myth really comes out of sticks and bricks type of claims, if you have a fire or something of that nature, that is true, carriers are always looking to do it most cost-effectively, not necessarily the best, but in this particular space at this time, it's in the carrier's interest to get the very best vendors vetted and approved, because as all of us know, there are many fly-by-nights out there offering services and they really don't have the bandwidth or expertise to deliver on the services that they're talking about. And so I strongly encourage our clients to leverage the knowledge and the resources that the insurance industry is putting behind vetting these vendors, because they do have a good housekeeping seal of approval that comes with that.

And you're also, at this point, able to leverage the insurance company's buying power on those services so you're not going to be getting taken over the coals by those vendors. So I encourage folks to do that. So before we wrap up today's episode, and you've been kind enough to come back to join us again, Dave, I did want to put one other question to you and I'll preface it by making a statement that you can either agree or disagree with, which is that, your chief information officer is the star witness in the underwriting process, and as mom always told us, "You don't get a second chance to make a first impression," do you agree or disagree, and why?

David Anderson: I would agree. I think it's true. If you work with a broker who's committed to driving high quality results and effective dialogue with the insurance marketplace, I would never allow my client to be put in a position to make a bad first impression. Depending on the complexity and size of risk, there should have been a number of fail safes, or circuit breakers to see where there realities around your cyber hygiene that we wanted to get ahead of and address proactively to control the dialogue? Was there something that maybe wasn't quite up to snuff on an application, or an event in your past that really you need to talk about?

It's important that you work with your broker when you're putting together your submission data, your underwriting data, to make sure that you have the upper hand in the discussion, because otherwise you're right, the insurers might, inadvertently most of the time, these people are trying to win business, Lynda, it's not like they're trying to turn business away, right? But they may put your CIO or CSO in a position where they're ill equipped to answer a question and you have then accidentally made a bad impression. So practice being prepared for the discussions that underwriters are going to have, frankly engaging a broker that does those things with their client is a differentiator. And yeah, I think first impressions are a huge part of your discussion with the marketplace.

Lynda Bennett: So Dave, you stole my shameless pitch in your direction, which is to talk about how important it is. These cyber policies are among, if not the most complex insurance product there is on the market today. And there are a lot of brokers out there, and I've worked with a lot of different brokers, and the importance of having a knowledgeable, dedicated insurance broker who is negotiating these policies every day of the week and twice on Sunday, I can't overstate the importance of that right now, not only on price, but also on terms and conditions, because as you know, there are still a wide variety of policy forms on the market, no two policies are the same, and the needs of particular companies in particular industries are also not the same. And so I agree with you a hundred percent. Getting those tech geeks prepared to talk to the insurance geeks takes a lot of preparation so that we get it right and communicate the information that needs to get communicated, but do it in an effective way so that the insurance company has a confidence and a desire to jump on board to ensuring this risk.

So, as I said, I really do appreciate Bridget and Dave, both of your time today, you've been gracious enough to agree to come speak with us in a subsequent episode here. So while we've given everybody a taste of what ransomware attacks entail and some of the things that you can do before the breach occurs to put you in the best position to respond to it, in our next episode we're really going to dive into once the unfortunate circumstance has arrived that your system has been breached, what are the things that you need to do to immediately respond to it and then also to maximize your insurance assets. So thanks again, and we'll see you real soon.

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.