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

**Episode 9 - The Ransomware Attack Part 2 – How To Respond When The Enemy Overcomes 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, Chair of Lowenstein Sandler's Insurance Recovery practice. In today's episode, we're going to continue our conversation with Dave Anderson and Bridget Choi, about ransomware attacks and how to respond to them, and maximize your cyber insurance asset.

In our last episode, we talked about the steps that companies need to take to prevent an attack from taking place, and to get cyber insurance coverage in place. Today, we're going to talk about the steps that companies need to take after they've unfortunately experienced a security breach, and received a ransomware attack.

Let's get right down to it, Bridget. It's Friday afternoon, I'm the head of IT, and I've just been told that our network is down and we've received a ransomware demand. What do I do next? Do I ask them if they want cash, check, or a credit?

**Bridget Choi:** The first thing I would do is inform everyone in your company, and keep a close guidance on this strategy, and the strategy should be go to your incident response plan. The first thing on your incident response plan should be contact your broker and report the claim to your carrier. Your carrier will help you get your vendor, they will get you your breach coach, and they will start dealing with the crisis in an appropriate manner, and in a skilled manner, that's absolutely necessary in this sort of attack and incident.

**Lynda Bennett:** All right. Dave, it looks like I've got to call my broker first. It's now six o'clock, we've found our cyber insurance policy. And, we see that Dave Anderson sent us the final package. What do we do next?

**Dave Anderson:** Yeah. I've generally found that it's always actually Saturday at eight AM, which is my least sunshine-y time of the week. But yeah, it's always important that you reach out to the broker. Obviously, you might have some resources that are on emergency standby that you're going, standing up. But, you should reach out to your broker so that they can reach out to insurer.

There's a number of different reasons why you should do that, but first of all, you want to make sure that any costs that you incur immediately serve to do what we call erode the retention, or basically chip away at your deductible. Most insurance policies in general won't let your deductible be eroded until you've provided the insurance company with notice of a claim. Every penny that you spend needs to erode that deductible, and that's not going to start until you notify the insurer.

Second, you want to notify the insurer as quickly as possible so that everyone is on the same page with the vendors that you're working with. If you're working with Kivu, for example, they're probably going to be on every insurer's panel and you're not going to have an issue getting an underwriter's consent to the hourly rates and the billing structure that Kivu has in place. If you work with someone that's a little different that may not be on your policy, you need to have the underwriter's consent before you incur those expenses. There's a lot of agita or heartache that comes in these claim situations when clients engage a forensics firm or a law firm that is not on the insurance company's panel, and cannot adhere to the insurance company's rates, that leads to, perhaps, potentially uninsured loss or the outright denial of the ability to use that firm.

The last reason you should notify your broker so that they notify your insurer immediately is that you do have a requirement to cooperate with the insurer and not prejudice their rights. Whether that's timely notice, or admitting guilt, or doing anything else that might impede the insurer's rights to their own capital under the policy, you want to always cooperate with your insurer. You're not compromising any sort of confidentiality, especially if you have a privacy law firm engaged already, to reach out to that insurer. But, what you are doing is everything you can to make sure that you've done everything that you're obligated to do within the four walls of your insurance contract, so that you're not jeopardizing coverage.

**Lynda Bennett:** And within the bounds of reasonableness, Mr. Anderson, they do have a duty to cooperate. But, it is within the bounds of reasonableness. All kidding aside, I agree with what you've said. In my experience, things tend to go a lot smoother when there is an immediate air of cooperation and collaboration in circumstances like this, rather than running too far down the road with your own vendors, your own counsel, and then trying to have the insurance company play catch up. Sometimes, we can have those situations work out okay in the end, but they're a lot more difficult than if you follow the process that you just described.

Although, I do want to ask one quick aside there, on the use of vendors in particular. I know the carriers like to vet who is going to be the outside vendors, and also who's going to be the law firm vendors. But, are there steps, if you have a particular vendor that knows your system really well, is there something you can do on the front end, so that when this crisis moment hits you're not getting into the fight with the carrier? Let's say, I want Kivu Consulting as my chosen vendor. Is there something I can do before I'm dealing with the breach to get approval for that?

**Dave Anderson:** That's a really good question, and it's important. We actually try to get ahead of it more so than we have in the past, because this is a real thing.

Let's just say that you wanted to work with Lowenstein Sandler as a breach coach, in the event that you have a cyber-attack. Lowenstein may not be on a given insurer's panel for whatever reason. The only thing you have to do is ask your broker to let your underwriter know, "Hey, our privacy attorney is Lowenstein Sandler. They've handled privacy for our company for 20 years, they know the firm, they know our policies and procedures. Can we please get them on the policy, endorsed onto the policy, as an approved privacy vendor?" It's no different than if you want to work with Kivu for a forensics vendor. If they're not on the insurer's panel, all you have to do is ask and they can get endorsed.

Two things happen when you do that. One, the insurance company will probably ask you to provide evidence of their competence in this specific field. I don't personally think that's unfair. And then two, the vendor that you're asking for will probably need to adhere, or try to fit into the mold of the billing and hourly rate requirements of that insurance company. I have had law firms that could not get to the hourly rate requirement that the insurance company required, so the insured made the decision to keep the law firm, but any costs in excess of the hourly rate the policy would pay would be bourne by them. That was invaluable to our client, because it was more important to retain the relationship with that privacy firm.

But, the short answer is it can be done, Lynda. And if you've got someone that you're already working with, it's probably going to be really easy to get them endorsed onto the policy instead of having to beg in the middle of a crisis on Sunday afternoon.

**Lynda Bennett:** Great. Well, thanks for that Dave.

Now, we've called the insurance company. We've got the $30 million ransom demand. And, the insurance company has told us, "Hey, call Bridget over at Kivu, because we're not just going to pay the $30 million demand." What happens next, Bridget? What happens after the insurance company's looped in, we've got this $30 million demand? What is the next step to take? And, if you can comment on the virtues of a quick payment, a prolonged process, and that lovable in-between space, that would be great.

**Bridget Choi:** I would say this is where being prepared for this situation ... A forensic vendor like myself, an incident responder, will gather all the information available, will find out the variant, will take an understanding of what assets have been affected. What are the viability of the backups? Can we recover? If we can, we'll get an understanding of is mission critical information impacted? Is it just cat videos? We don't really care if it's cat videos, we can recreate those. Is what was impacted, or exfiltrated in certain circumstances, valuable to the company, and how valuable it is? Because, particularly with a $30 million demand, what you're going to have to do is make a very detailed business decision in a short amount of time.

Think about this. You're going to have to weigh whether attacker who has attacked your company is potentially an OFAC sanctioned entity, or connected to an OFAC sanctioned entity? If they are located in Iran, if there's threat intelligence to say the people who control them are on the SDM list, you may not be able to pay. That is one of the factors you're going to look into, who are they. And then, the next factor is what is the benefit of paying this attacker. If we can get them down 20%, is it still worth it? If we can get them down to 1%, 10%? What do we know from threat intelligence and other incidents that we've handled, about the negotiations and our strategy? It's not a binary decision.

The decision has many weighted factors that they're going to have to consider, and it's going to be different every time. If I tell you the $30 million I handled last week is going to far different than the one I handle next week, because they don't come the same way, each variant acts very differently. Going back to my original thought, preparation is everything. Knowing your assets, and going with the right vendor, and the right breach coach who can guide you through the circumstance is crucial.

**Lynda Bennett:** That's great Bridget, I appreciate that.

Dave, I've got to ask the question that every single one of my clients who’s unfortunately been in this situation asks immediately. Are you telling me the carriers will pay an extortion demand? How is that possible, that you can get insurance for that?

**Dave Anderson:** Yeah. I mean, that's been the question of the last six months. In a boring insurance rag about 12 months ago, I was quoted as basically accusing the entire cyber insurance marketplace of "feeding the monster." While that was not a favorable way of quoting me, it is somewhat true. We have existed so long with the ability to leverage an insurance policy to pay a ransom, and I think the secret's out which is why we've seen inflated ransom demands, we've seen companies that think that the insurance policy is going to be their ultimate safety situation. That's not the case, I don't think it was ever intended to be the case, although we've learned some lessons along the way.

Your insurer will work with your breach council and your vendor to come up with a "team conclusion" around whether or not your systems can be restored,

or whether or not a ransom has to be paid. That's also assuming that you can pay the ransom, because they're not an OFAC sanctioned entity. Then at that point, your insurer will then, ideally, give you consent to pay the ransom and you can try to get a key to decrypt your files. My experience has been that the decrypters are usually not as effective as you hope that they are. The ransom can sometimes come back with a secondary demand, or a third demand in some cases, a few weeks or months later.

The insurers have really gotten away from immediately consenting to pay ransoms, and frankly, they are starting to push a culture where the ransom should not be the first line of defense. It should be backups, it should be isolation of the compromised workstations and endpoints. The ransom should really be treated as the last ditch effort to get back online. You saw that with the DFS update that came out a few days ago, in the state of New York that was just talking about how we should not be looking at it this way anymore.

The short answer is yeah, your policy can pay the ransom but it's gotten a lot harder to use that as your first line of defense lately.

**Lynda Bennett:** Yeah, that was the question that I was going to ask. Which is, how long can we keep this status quo? How much longer are the insurers going to have an appetite to insure that risk, when we're seeing these ransomware attacks proliferate every industry? And, the size and scopes of the ransoms are going up. That, to me, is an interesting issue to watch, whether we're going to see sub-limits, or the willingness to cover that disappear entirely on these cyber policies. That's just something to keep an eye on.

Bridget, tell me, after we pay the ransom, some of the claims that I've been involved in, during the negotiation process the bad actors will promise you that they'll deliver the encryption key. And also tell you, like every magician, we want to know how did you do it. Do you get to find out after you pay these ungodly high ransom demands? Do you get a window into how it happened, from those bad actors? So that you can take the steps to make sure you're done, and you're not going to be having your doorbell rung another six months from now by these guys, or the next band of actors.

**Bridget Choi:** I can tell you, sometimes and sometimes not. I will tell you that they're using tools that disguise them in the system, they wipe evidence, they wipe shadow copies of what they're doing. Often times, a lot of the evidence that should be there isn't there.

There's a whole sector of cyber call penetration testers, and what they do is they find vulnerabilities in the system. And, really what that is hackers. They're white hat hackers that you hire to find the holes in your security architecture. They have tools that they use to hide what they're doing. The bad guys are using the same tools, literally. Sometimes, you may know. And sometimes, no matter what we see in the system, there's no forensic evidence to suggest how this attack happens.

It's very frustrating for clients who, they just want to know what happened, and they want to know how they could happen to them. We could give some pretty good general ideas, but we may not be able to say, "The patient zero is this person. It's Ann from accounting who clicked on a link," or, "It's John from IT, who left the RDP open." Because they really, really are getting quite good at hiding what they're doing.

**Lynda Bennett:** Thanks for that.

In the couple of minutes we have left, Dave, I would like to talk about a few of the other coverage grants. And just touch on, at a very high level, some of the issues that I come up a lot with in my practice, which is obviously the cyber policies, the ransomware coverage is one element. But there's also, obviously, costs associated with patching the source of the breach. Are all of my costs that I incur there covered, including when, as part of my patch process, I upgrade from the Hyundai to the Caddy Escalade?

**Dave Anderson:** That's a really good question. The answer is unfortunately, it depends. I can see into the future right now, Lynda.

**Lynda Bennett:** You sound like a lawyer, Dave. Keep going.

**Dave Anderson:** Yeah, I know. Here we go, it's going to get even better. I can see into the future, because I can see all the underwriters that are going to listen to this podcast and cringe at me when I saw what I'm about to say. But, here we go.

There is a challenge around an insurance policy wanting to respond only to a fortuitous event and to make you whole, not better off than what you were beforehand. That exists in all types of coverages. Generally, insurance is there to get you back to where you started from, not to get you to Escalade because you've totaled your Hyundai.

That being said, there are certain inevitabilities that may not be able to be avoided, in terms of expenses, after a cyber-breach has hit. Lynda, you hit it on the head. If I'm running a legacy version of Windows Server that's not supported, or if I'm running Windows 7 on my endpoints, there are inherent vulnerabilities in those platforms because they're no longer supported that would make any victim of cyber-attack or data breach a target on an ongoing basis. A mark, as we would call it on the streets here in New York. It would be ideal for the victim of such an attack to upgrade the software to the most recent, or most basically patched and supported software version.

A lot of properly placed policies will either allow for commercially equivalent replacement language, which means that if the software that needs to be replaced because it was damaged in a cyber attack is no longer available, the insurance policy should pay for the commercially equivalent software, or hardware in some cases, available to you at that time. That is a fine line

between betterment and just getting the insurer back on their feet, which is always a challenge that we're finding in the insurance marketplace. Betterment really being the concept, are you going to get a new Escalade because you totaled your Hyundai. You can pay additional premiums for having the insurer provide an enhancement to the policy, that will provide usually a percentage of the policy's proceeds to betterment if it's crucial to get you back online.

But, at minimum you would always want to have commercial equivalent reasonable language to avoid the discussion around having the insurer come back and say, "We're not paying for upgrades. It doesn't matter what happened or why it happened, if you can't get a copy of Windows 7 for all your endpoints, then that's too bad and it's not on us."

It's important, also, to mention in terms of what's covered expense versus not covered expense, it's important that you work closely with your breach coach, your privacy counsel, and your broker in any claim situation. It's not to say that we would ever want to put a gun to the insurance company's head, but there has to be a commercially reasonable decision made on the claim, regardless of whether or not the black and white of the policy tolerates for buying upgraded software solutions. Because, if I can't get my system back up and running because I can't rely on my insurance to pay for that upgraded software, even if it's just one generation further, guess what? We're still going to have business interruption loss.

There has to be a team effort. I have always found that the insurance companies that we do business with have made the right choice and done right by the client, it's just a matter of having the dialogue and having a discussion around managing everyone's expectations. That's not to say that everything's going to be covered all the time, but I think that if there's a case to get people back online, you can usually get the insurer to help out with it, in that situation.

**Lynda Bennett:** Great. Another element, as we know, of these policies, and another element of responding to these types of attacks, frankly, is the regulatory and notification issues that flow from a breach. And, especially if personal information, employee information has been exfiltrated as part of the security breach. Just give me a minute or two, Dave, on the state of play of coverage for that under these policies. Are there any limitations around that coverage? Or, is the policy going to cover all of the attorney's fees as well as the costs associated with notification, credit monitoring for those impacted by the breach?

**Dave Anderson:** Sure. Every cyber policy should cover notification to affected individuals, or suspected affected individuals. All cyber policies should cover the cost to provide credit monitoring and identify theft restoration services, and should provide some allowance for voluntary provision of those services to victims in an effort to show good faith or avoid a claim. All cyber policies should have the privacy regulatory insuring agreement included when you purchase that policy. And if it is included, that policy should always include costs for defense, so the

costs to engage a privacy attorney to deal with a GDPR regulator, or a HIPAA regulator, et cetera.

The fines and penalties around privacy regulatory issues is much more difficult. I will tell you that most policies, the best policies in the marketplace, will affirmatively grant coverage for privacy regulatory fines and penalties, so long as those fines and penalties are insurable. That's really where the discussion comes into play, around insurability, whether or not a given statute allows for insurance. We don't always have a solid answer around that, especially around GDPR and some of the up-and-coming privacy rules.

But, if you can get the broadest language on the front end, you're probably going to have better odds post claim.

**Lynda Bennett:** That's great. All right, we're just about out of time. But, I'm going to give Bridget the final word, and it's going to be the cautionary tale. What's the biggest single mistake that you've seen a company make in responding to a ransomware demand? And, how would you correct that mistake?

**Bridget Choi:** I think the biggest mistake I've ever seen is folks who have a knee jerk reaction to ransomware, and won't listen to their consultants.

Just to unpack that a little bit, we talked about before, all of the factors. But, what they don't really want to hear is, "Okay, if you get that key, we know on this variant, all of your data might not be there. It may incur in your favor not to pay." Or, a lot of what we saw in 2020 was the bad guys take your information, and what a lot of these companies are paying for is the temporary relief from embarrassment that the bad guys took your information and are going to publish it. That's not a good reason to pay a ransom payment. That's not a good way to relieve yourself from extortion, because they're promise not to publish is not worth anything. There is no reason to pay in those circumstances.

The biggest mistake you can really make is not listening, and not pushing your attorney and your vendor to give you all the information available so you can make a really informed decision on whether to pay, because it isn't something that you want to take lightly.

**Lynda Bennett:** That's great. I appreciate the insights that both you and Dave have provided to us, both in today's episode as well as our earlier recorded episode. Tremendously appreciate your time, your insights, and obviously your expertise. But most important of all, I appreciate you keeping it real and in line with our motto here at Don't Take No For An Answer, which is to keep it practical and in plain terms.

Thanks for joining us today. Hope you enjoyed the episode, and we'll see you next time.

**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. 