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

Episode 40
The Significance of Operational Technology in Cyber Insurance Underwriting – Part 2

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. And today I am very pleased to welcome back two of my guests, Shiraz Saeed, who is a Vice President and Cyber Product Leader for Arch Insurance, as well as Rob DiRico, who is the Cyber Liability National Practice Leader for Arc Excess and Surplus Insurance. So welcome back Shiraz and Rob, thanks for coming back to discuss cyber insurance yet again.

Shiraz Saeed: Thanks for having us Lynda.

Lynda Bennett: Right. So in our last episode, we were talking quite a bit about the cyber market with a particular emphasis on privacy concerns. So today we're going to focus a bit more on operational technology issues, as well as the role that regulators are playing in having companies focus more on their cyber insurance and cyber hygiene, or privacy and security hygiene. So let's kick it off with that operational technology issue. Shiraz, why don't you tell us how insurers are looking at that and assessing risks through that lens?

Shiraz Saeed: Sure, absolutely. I think it's a great question and a lot of times, again, as I've said, I've been underwriting cyber risks for a while now, and it's always really revolved around privacy, which was always the major concern. But over the years, especially over the past two years with the increase of ransomware, we've seeing that the reliance on operational technology by every class of business has increased dramatically. And post COVID, it's increased even more. Just think about how many companies went to remote working instantly overnight, right? The carrier I worked for before I came to Arch, everybody was in the office five days a week and working from home was a non-starter. And then, overnight, everybody was working from home, right? So that connectivity and the access and the need to be able to connect through the computer network is more important now than it's ever been in history.

Shiraz Saeed: And if your system's not available for hours or days or weeks, how does that impact your business? So the first thing that we would start looking at is

trying to get the applicant to identify critical platforms, applications, or systems that they use to rely upon to operate their business. Once they've identified them, we should then think about two things. One: What's the business impact if it were to go down? And the second thing we would be thinking about is, do we control this platform application or system ourselves, or do we rely upon someone else to operate it? All right. Then we have to think about how do we secure this and is it properly secured? How do we separate this from the information network system so if one thing gets compromised, it's not both of them getting compromised. Is this application platform or a system at an end-of-life stage? Is it still supported? And what redundancies do we have? Can we work offline? Do we have a backup application platform or system that we can rely upon if this one were to go down?

Shiraz Saeed: So these are some of the things that we are thinking about that are very important when it comes to this operational risk. Because our claims data shows that there is an on-demand business model, where if we don't get the product on-demand, we will lose the sale and ultimately lose the profit or the income. And because of that, it's super important to think about all of these applications. And then a lot of them will be through third parties, and that's the other piece of it where most reputable carriers in cyber are extending the business income loss or the business interruption to third parties. So one group would be like a technology contractor. So that's an IT company that's providing you services.

Shiraz Saeed: And then the other group could be defined in many different ways, but ultimately it's any other organization you rely upon to conduct your business. This could be a supplier of goods, products, or services, a receiver of your goods, products, and services. So the example that I would give is let's say we wrote a hotel and the company that provides the sheets and the linens and all those things happens to suffer a ransomware. And now we can't change the sheets and those types of things. Does that knock the company out for a day or two, right? And then how much did we lose? So these are the types of things that we are thinking about when it comes to underwriting to that operational loss.

Lynda Bennett: I can bring it closer to home. Certainly our law firm functions, or is heavily reliant on, technology, access to our email, access to our documents. And I know that there's been an increase in focus among the cyber criminals on shutting down businesses like ours, and our billable hours are our life blood. So we're doing lots of training. So Rob, go ahead. What other inputs do you have there?

Rob DiRico: In terms of also high risk management hygiene, you also have to think about vendor relationships and partnerships and supply chains. So I have a good example: you could have a company's network security be in tip top shape, like Fort Knox, but if they have vendors gaining access to the network, you also have to make sure the controls are applicable to vendors when they log on and what protocols they have in place. So for example, the vendors logging on to use a certain platform that the company's providing, like Shiraz mentioned, are they using MFA to get in, too? Are they following the proper protocols? What are the indemnifications between the two entities?

Rob DiRico: I've had a situation where we have a very large company that has a portal for all their vendors to go on and buy components and parts. And those vendors have respective vendors who also utilize their respective services. And I've had a breach where our client was compromised, which then went downstream and the computer virus went to their vendors and their vendors' respective vendors. And then the lawsuit came in because the nexus of the breach happened with my main client. However, there are defenses for my client's network security, and each respective downstream customer should have their own protocols in place to prevent that intrusion of their network to stop it from happening. So the liabilities kind of get shifted and minimized downstream as you go, but there's also indemnification requirements and subrogation requirements. So, the best clients are checking that and seeing who are we indemnifying? How does our insurance policy apply to them?

Lynda Bennett: Right. And also priority among your insurance policy and the supply chain partners policies. This is something that we spend a lot of time educating our corporate lawyers on because insurance provisions, indemnification provisions in these supply contracts tend to be a box checking exercise. And then all of a sudden the loss happens and even the insurance requirement of you have to have a media policy. Well, I meant that you should have had a cyber policy when I said media policy. And you have corporate lawyers that don't know the differences in the nuances. And so, yeah, I agree. It's a very important area.

Shiraz Saeed: Lynda, can we ask you a question?

Lynda Bennett: Sure.

Shiraz Saeed: How often do you see that an SBA or an MSA master service agreements, service business account agreements, these agreements, that they actually define what cyber is, what is network security? They actually define private information and then say, if one of these two things were to occur, this is how we think we will proceed. And oh yeah, you should also have insurance that covers like, have you seen it like that often?

Lynda Bennett: It's rare. There's starting to be more attention paid to it, I would say in the last year or so, but prior to that, you wouldn't even see cyber insurance on the list of required insurances in the agreement. And if you did, again, it would be a Frankenstein butchered reference to what type of policy actually needed to be in there.

Shiraz Saeed: On the carrier side and the broker side. And I guess the legal side as well. We have clients on both sides of the fence. We have clients that are providing the services that are the actual professional services companies. We also have clients that I would refer to as the users. And this contract, depending on what side of the fence we're sitting on, we're going to change, right? So if we are professional services company, we're advising them don't indemnify them for anything. Don't even bring it up in the contract, leave it be. But when we're the user, we're going make sure they define it, make sure that you have the right insurance, make sure they're going to indemnify you. Make sure you're doing everything. So what happens is when I mention the aggregation about the MSP and others is when you write the MSP and you

write 10 of their customers, well, now you're sort of in a little bit of a pickle. Who's paying who and who's subrogating against who, where?

Lynda Bennett: Right? No, exactly. And when we train our clients on this and our corporate lawyers, it you're exactly right, Shiraz. Depending on whether you're giving or getting that indemnification, it's either going to be as broad as all get out or as narrow as nothing. But you're right. When you're on all sides of the deal, you get to just pick which pocket out of your own pair of pants you're picking the money out of.

Rob DiRico: My favorite is when the client comes to me and says I need a certificate and I have to be primary to any other policy. You're an additional insured. I have to wave my subrogation rights and there's 27 insurance. Oh, and we [inaudible 00:10:33] infringement coverage too. It's like they throw in the kitchen sink. And you have to vet that to make the policy will give that coverage or endorse it so it's challenging.

Shiraz Saeed: I just wanted to give a message for the audience - identify the vendors, make sure they have the security that you have, check out those contracts and make sure you have the right stuff in place.

Lynda Bennett: Absolutely. Spot on. So I want to shift gears. We're all watching in horror what's going on in the Ukraine. And so there's been a lot of chatter about the war risk exclusion. And I'm sure both of you are familiar with the Lloyd's of London pronouncement that they're just not going to provide coverage for certain types of risks under that war risk exclusion. Is London an outlier there, or do we see that there will be coverage and you're going to have to really carefully parse those words of that war risk exclusion?

Rob DiRico: I would say from a broker standpoint, Lloyd's has definitely shown that, they're adding it to their excess policies too. Even if the primary insurance policy that they're following has language related to war, they want their own wording. I think that this is evolving. I think many carriers have an outright war exclusion now with exceptions to cyber terrorism. I think as this continues to shift, I have a little bit of a fear that when we have a breach and the forensics report that it's coming from the Russia area, they might try to overreach a little bit and say that it arises out of war. Certainly you have the OFAC issue now.

Rob DiRico: Let's take war aside now. There's a lot of sanctioned entities now that you can't pay a ransom to without getting penalized by the federal government. And insurance companies and the law firms that are hired to negotiate the ransom, they check that and vet these entities to see if they're sanctioned out and give their testament before the insurance company does anything. Now with all the sanctions on Russia, it's not just the war exclusion you have to worry about. Let's say you don't even bring up the war exclusion. They could say that this is a sanction related entity or country, we're not going to pay. I feel like it might start coming to the insurance company side, Lynda, in the U.S. And I think that we might see some moving in language, but I would say this, there is a buyer beware, but seller beware.

Rob DiRico: What kind of a precedent would it set for an insurance company to invoke an exclusion based upon war when you really are going to have a hard time getting right down specifically to proving that it was from the Russian military. How are you going to do that? So watch what you're doing because a lot of your policy holders are going to move their business if that happens. So it's going to be interesting to see what happens.

Lynda Bennett: Yeah. You hit the nail on the head, Rob, for me, it's what is war? We used to know what that was. It was charging a hill. It was flying into restricted airspace. Now knowing who was really behind something that happens in cyberspace, and you're exactly right as a policy holder lawyer, I'm going to be reminding every court that this is an exclusion and the insurance company has the burden of proving that exclusion and finding the facts to prove that exclusion. It's going to be, I think, a murky place for all of us to go.

Rob DiRico: Yeah, show me it's the third brigade of the cyber liability unit of the Russian [inaudible 00:13:54], and then we could talk about it being war.

Shiraz Saeed: Obviously this whole conversation that we had this episode and last episode are my opinion as Shiraz, an individual, and do not reflect the opinions of Arch Insurance Group. And I reemphasize that again now when we discuss this topic. This has nothing to do with Arch's policy, form or anything like that. Okay.

Shiraz Saeed: In general, I personally believe this term cyber terrorism is not the right term to describe what we're trying to say. What we're trying to say —and if you do the research on this, you're going to come to realize that a large portion of the activity in the cyber space in terms of intrusions and incidents—, can be or possibly could be attributed back to some sort of state sponsored action. So if it is state sponsored or it's an individual or group of individuals acting on their own, a criminal organization. Well, what are they both doing? They're both going after a computer system and trying to disrupt it, attack it, whatever it may be. In a standard cyber policy from a reputable carrier they never actually ever identified who the actor is. They just say if the computer system is impacted.

Shiraz Saeed: So somebody came up with this idea that we should define this term cyber terrorism, and connect it back to an individual or group of individuals with some sort of motivation or intent, political, ideological gain, whatever. But Lynda, as a coverage expert, you would know it's about the trigger and it's about the result. So the trigger is: was there a security failure, a network security breach? Yes, there was. Well, what was the downstream impact? Was it connected to, arising from, or related to a war, a war-like operation or a military action? Did it result in bodily injury or property damage? Or did it result in data exfiltration and a general business interruption?

Shiraz Saeed: And I think that third group of nonphysical related acts is where a lot of carriers can be comfortable.

Lynda Bennett: Devil's in the details always.

Shiraz Saeed: It's the war and the bodily injury and property damage that everybody's trying to avoid. You mentioned earlier, Lynda, that war meant physical. And that's the question. Our cyber policy is designed to cover nonphysical. So we have a big BIPD exclusion. Nobody's talking about that because their concern is the nonphysical.

Rob DiRico: Good point.

Shiraz Saeed: So what is the example there? Like Rob was alluding to, let's say we write a company here in the U.S. that uses a Ukrainian software company to do their back office, electronic medical records and scheduling and booking. Rob's client is this healthcare company. They call Rob frantically saying we haven't been able to access the network for days. We keep emailing and calling the company and they're not responding to us. Then Rob asks where's this company based? Uh, Ukraine. Really? Okay. Why are they not responding? Did they evacuate the building? Was the building blown up? Was the material confiscated? We don't know. We just know it's in the zone. And now the question becomes: is this enough to attribute it to the war? Right?

Shiraz Saeed: So what we're starting to see, and Rob, you could speak to this if you've seen it, I've seen it, some carriers are now creating a specific area exclusion where they'll mention Russia, Belarus, and possibly Ukraine, and if it arises from this area, it's excluded. You've seen that?

Rob DiRico: You're starting to, but I haven't seen on a specific cyber policy yet. I've seen it on every other policy now.

Shiraz Saeed: I've seen it on a couple because we do write access, and that is another direction that you can go in, which is different than war.

Lynda Bennett: Well, we've got just a couple of minutes left here so I want to touch on the regulators and they seem to be hyper focused right now on cyber insurance and raising privacy and security awareness among companies. How is the regulatory activity impacting the placement of cyber insurance policies?

Rob DiRico: I would say that biometric information has become a very big concern of insurance companies as people are now putting thumb prints and certain types of biometric identifiers as part of their everyday process of coming to work. Insurance companies now are requiring supplemental underwriting applications to see if a company stores or collects biometric information. And they vet that to see if they're compliant with certain guidelines before they afford the coverage for that. You will see certain carriers and a biometric privacy act exclusion if they feel like the company's not doing the proper protocols, and you have to compare that to other policies that might cover it for claims by employees.

Rob DiRico: So for example, employment practices policy should cover it. However, if they both exclude it, you have a problem. And a privacy policy on its face, generally speaking, without any additional exclusions, typically the definition of privacy law that covers a regulatory related coverage, would trigger it. But depending upon how the policy is worded, you might have to have it covered if it stems from a breach or if it comes directly from an employee, if there's no

specific exclusions, you can get that coverage. So I would say it's being vetted more because the policies have responded to biometric claims, in my experience.

Shiraz Saeed: I want to, cognizant of time, Lynda, I want to give you a quick one to two minute answer on this, and then I guess we can conclude. So one, what Rob is mentioning broadly is referred to as wrongful collection coverage. It's more about how you collected, gathered, transferred, transmitted, sold the information than it is about losing the information. And it's most commonly seen through the Biometric Information Privacy Act, BIPA in Illinois. All right. So we need clients to think about their collection disclosure and consent.

Shiraz Saeed: The second thing regulatory concern is right now or what we need from regulators, is relating to controls and creating a standardized level of controls that all American businesses need to have. I would equate it to la building department for fire insurance in the past. Every building that's made, there's a certain code that has to be held. All computers that are going to be used to operate and use a business should start establishing a code of security, minimum standards, that everybody needs to adhere to. And that's a public private partnership between the insurance carrier and regulators. Right now it's starting with awareness and notifying regulators of what's going on, but we have to move in that direction.

Shiraz Saeed: And the other example I would give is sort of like the auto industry. A rear view camera was something that was optional in the past, but now sort of mandatory, same with seat belts and other things. So as the risk evolves, we have to come up with the right way to minimize the risk and then incentivize people through regulation to move in that direction.

Lynda Bennett: I think that's great and a great way to end. The way to bring stability to the cyber insurance market is for everyone to be a better risk and to be more secure and to keep the claims and losses activity down. And that's the way to do it. I want to thank you both for joining us today, as well as in our last episode. Certainly there's lots to discuss. This is going to continue to be an evolving market. I really appreciate you both sharing your knowledge with us today. And we'll look forward to having you back again soon. Thanks so much for joining us.

Shiraz Saeed: Thanks Lynda.

Rob DiRico: Thanks 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 and 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.