Lowenstein Sandler's Cybersecurity Awareness Series

Session 6 -
Cyber Insurance Changes in the Aftermath of Log4j

By Lynda Bennett and Ken Fishkin
APRIL 2022

Ken Fishkin: Hello, and welcome again to another addition of our Cybersecurity Video Series. I'm Ken Fishkin, Manager of Information Security here at Lowenstein Sandler, and I'm here today with Lynda Bennett, who is the Chair of our Insurance Recovery practice.

Lynda Bennett: Thanks, Ken, pleasure to be here today.

Ken Fishkin: Pleasure. Let's start with talking about the state of the current cyber insurance market. And the first question I want to ask is: what impact has log4j had on the insurance market?

Lynda Bennett: So, we saw a couple of impacts. Immediately following the breach, we had a number of insurance regulators immediately issue bulletins, reminding companies of their breach reporting obligations and to remain vigilant and focused on risk mitigation—measures that they should be taking. But the much broader impact, and harder impact of it was, it was really another body blow to a market that was already feeling a lot of impacts and breaches and losses, particularly COVID-19. As we know, when we had to convert to remote work over night—that created a field day for cybercriminals to start accessing companies. And they did—we had Solar Winds, we had Microsoft Exchange—so this was really the cherry on top of a very bad, ugly sundae to look at for carriers.

So we saw some of them just leave the market entirely and say, you know what? The losses are too many, too significant. We're not writing this business anymore. For those carriers that decided to stick around, what we've seen is surging prices. I mean, we're seeing incredible, year-over-year premium increases. We're seeing self-insured retentions or deductibles going up significantly. We're also seeing a restriction in terms. So, one concrete example of that is we're seeing a lot more sub-limits. So you used to have a $5 million policy and no matter what type of loss you experienced, the full $5 million would be available for you. Now, social engineering and fraudulent instruction losses are very much on the rise. The insurers are responding to that by putting a sub-limit on it, saying ‘we'll cover you for that, but only up to $500,000, not the full policy limit.’ And we're also starting to see more exclusions creeping into these policies. And particularly for this most recent breach relating to denial of service vulnerabilities, we're going start to see some exclusions come on for that.

Ken Fishkin: Interesting. That's definitely what's going on in the cyber world, the denial of service attacks that we've been seeing. What do you think are the two biggest threats that are driving the insurance prices to skyrocket?

Lynda Bennett: Definitely poll position are ransomware claims. The reason for that is, a couple years ago, those were five-figure ransom demands or cyber extortion demands that were made. Then we moved into six-figure demands. Now we're into very healthy seven-figure demands, and, depending on the size of the company, we're at eight-figure demands. My observation is the criminals are getting a lot smarter and more targeted in the companies that they're breaching. Many of our viewers are probably familiar with a large insurance company that got hit a couple of months ago, and what do you think they were looking for, Ken?

Ken Fishkin: They were looking for what clients they had.

Lynda Bennett: That's right—what clients had purchased cyber insurance and what limits did they buy, so that that could help inform what the next demand is going to be. And that really sent a pretty significant ripple through the market as well, and concern that these losses are just going to keep coming and coming. So, ransomware is number one, for sure. And then number two is the impact on supply chain. Because, as we saw from this most recent breach, this was a widely used software product and it hit every industry of its vertical. So the carriers, when one company goes down, you can have this domino effect down the supply chain that is going to triple, quadruple, the losses, just like that.

Ken Fishkin: I know from purchasing insurance for our own firm that the rules have kind of changed. Before it used to be that, as long as we had good backups, we were patching, we had antivirus on, that would be considered good enough to get insurance. But now I know that insurance carriers have really put new requirements on. Can you give our audience one example of that?

Lynda Bennett: Yes. The number one thing that cyber insurers are going to be asking about during your underwriting process is multifactor authentication.

Ken Fishkin: For those that don't know what multifactor authentication is, it's something like a password, something you have, like your fingerprint or facial recognition, and something you have, like your cell phone. So if you ever worked with a bank where they send you a code after you type in your password, that's called multifactor authentication. And it's going to take companies a lot of time to change their practices, to make sure that they have that on their critical systems.

Lynda Bennett: And so where the insurers are really focused on relates to how are your employees in this new work-from-home environment that's here to stay on some level—how are your employees accessing the system when they're not in your workspace and more important, I would say most important of all, is they're really focused on email, when you're accessing your email from non-corporate-issued devices, is that MFA in place? Is it really going to be

protected? Because that's where the source of a lot of these breaches trace back to.

Ken Fishkin: Interesting. Now what's a small business to do who doesn't have all the resources at hand to implement all the changes that need to be done by these requirements that insurance companies are requiring?

Lynda Bennett: So a couple of things. The number one thing I think is most important for every company is to make sure that you're working with a cyber broker that specializes in placing cyber insurance policies. Not every broker is in the weeds on what the state of the market is today. What is the right policy form, given your business model, given your risk profile? So really being aligned and having an advocate in the market for you that understands your business and what your risks are. Another really important thing is to have those contingency plans in place, know where your records are, know where your cyber insurance policy is, because at 5:00 when this breach happens on a Friday—which is usually when they do to create the ultimate chaos—not being in a position to nimbly get in there and respond is not going to make you an attractive risk to an underwriter looking at you.

Lynda Bennett: So, knowing where your documents are, having your Chief Information Officers who are going to participate in those underwriting calls, having them prepared to be ready to answer questions. I in fact myself as an insurance geek, being a cyber geek and being able to speak to insurers, a couple of different skill sets there. So get your people prepared. Mom always told me 'you don't get a second chance to make a first impression,' and that's never more true than it is today in the cyber market. When you're talking to underwriters to show that you're a good risk.

Ken Fishkin: Thank you. That's very helpful. What's your take on how Lloyd's of London got out of the cyber insurance business, as far as dealing with nation state attacks?

Lynda Bennett: That's pretty big news. I think that it's going to engender a lot of coverage litigation, unless other carriers follow a suit and just say 'we're not covering any act of cyber war.' But in the short term, we've already seen some coverage litigation around the war, exclusion in a cyber policy, and what's really hard to pin down in this particular space is what is the 'act of war'? You know, when we think about war, we think about traditional 'I'm going to charge that hill', 'I'm going to fly into that restricted airspace and take an aggressive act.' It's a lot harder to pin down those facts in cyberspace. And the good news for policy holders is that the war exclusion is an exclusion. So the insurance companies bear the burden of developing that factual record, that this was an act of war that it was, not just a terrorist, but that some nation state claims credit for that act of war. So it's going to be very interesting to watch, to see if other carriers follow suit. It's also going to be interesting to see how the courts resolve this issue. Again, keeping in mind that it's the carrier's burden to prove that, and these facts are pretty hard to pin down.

Ken Fishkin: Thank you. All right, I get it. Now, can you give us one final thought for policyholders to look at when they're renewing their cyber insurance?

Lynda Bennett: If they want to read cyber insurance contracts, I'll have to give out secret decoder rings. These are some of the most complicated insurance policy forms that are on the market today. But it is actually my parting piece of advice: read and understand those policies before you have a breach. As I mentioned before, there's tremendous variation in the market right now on what the terms and conditions of those policies are. The devil is always in the detail in an insurance claim dispute; the words matter. And so waiting until after you've had a breach is surely going to lead to unwelcome surprises. These policies can be negotiated when you've got the right team in place. You can negotiate some of these terms and conditions, but more important, is understanding what's within the bounds of coverage and what's outside of the bounds of coverage before you have the claim is going to put the company in a much better position.

Ken Fishkin: Thank you very much, Lynda, it's been a pleasure, and thank you for joining us for another edition of our Cybersecurity Video Series.

Lynda Bennett: Thanks, Ken. I appreciated the time today.