Podcast

What to Look for in a Cyber Insurance Policy

By Joseph J. Lazzarotti

October 20, 2023

Meet the Authors

Joseph J. Lazzarotti

Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Related Services

Cybersecurity Awareness Audio Guide
Privacy, Data and Cybersecurity

Details

October 20, 2023

Guest speaker: Marc Schein CIC CLCS

In today's data-driven world, cyber liability insurance has gone from a good idea to essential coverage for organizations. As a result, it is imperative that organizations are familiar with key elements of their cyber insurance policy to ensure proper coverage for potential loss and damage.

Jackson Lewis P.C. · What to Look for in a Cyber Insurance Policy

Listen on Soundcloud
Listen on Apple Podcasts
Listen on Spotify
YouTube

Transcript

Alitia Faccone:

Welcome to Jackson Lewis's podcast, We Get Work. Focused solely on workplace issues, it is our job to help employers develop proactive strategies, strong policies, and business-oriented solutions to cultivate an engaged, stable and inclusive workforce. Our podcast identifies issues that influence and impact the workplace and its continuing evolution and helps answer the question on every employer's mind, "How will my business be impacted?" In today's data-driven world, cyber liability insurance has gone from a good idea to essential coverage for organizations. As a result, it is imperative that organizations are familiar with key elements of their cyber insurance policy to ensure proper coverage for potential loss and damage. On this episode of We Get Work, we discuss what organizations need to know when obtaining cyber insurance to best minimize risk. Our hosts today are Joe Lazzarotti, principal in the Berkeley Heights office of Jackson Lewis, co-leader of the firm's Privacy Data and Cybersecurity Group, and Marc Schein, national co-chair of the Cyber Risk Practice at Marsh McLennan Agency.

Joe is a certified information privacy professional with the International Association of Privacy Professionals and focuses on the matrix of laws governing the privacy, security and management of data, as well as the impact and regulation of social media. Marc is a certified risk manager, certified insurance counsel and commercial lines coverages specialist. He assists clients by customizing comprehensive commercial insurance programs that minimize the burden of management experience, including cybersecurity, cyber insurance, technology, E&O, directors

and officers, practices, liability errors and omissions.

Joe and Marc, the question on everyone's mind today is, "What should an organization look for in cyber insurance coverage, and how does that impact my business?"

Joe Lazzarotti:

Okay, good morning or good afternoon, wherever you are, and thanks for joining us for the next installment of our cybersecurity podcast series. I'm Joe Lazzarotti, I'm a principal with Jackson Lewis, national law firm with locations around the US, located here in our Berkeley Heights, New Jersey office. I have the pleasure of collating our firm's privacy data and cybersecurity practice group. We work a bunch in our group with cyber insurance, so it's an important issue for us. I'm really grateful to have Marc Schein with us today to help us navigate some questions our clients have about cyber insurance. Marc is terrific. He's the national co-chair of the Cyber Risk Practice at Marsh McLennan Agency. Marsh McLennan Agency is a subsidiary of global insurance brokerage Marsh, providing business insurance, employee health and benefits, retirement and private client insurance solutions to organizations and individuals.

Marcus' clients, by customizing comprehensive commercial insurance programs that minimize the burden of management experience includes cybersecurity, cyber insurance, technology, E&O, directors and officers, employment practices, liability and errors and omissions, quite a level of experience, Marc, thanks so much for being here today. I really appreciate it.

Marc Schein:

Absolutely excited for the talk, Joe.

Joe Lazzarotti:

Awesome. So let's just jump right in. So cyber insurance, a lot of folks talking about it. It has taken its place among the coverages most organizations find essential in today's data-driven world. With that, many organizations still may be unfamiliar with aspects of this coverage. They know they need it, but they're just not sure what makes sense for them, how to approach it. So Marc, maybe a place to start is, can you speak generally, what are things that a company might want to start thinking about as they approach getting cyber insurance for their organization?

Marc Schein:

So really from a starting point, thinking about if you're a first time buyer or if you've been buying cyber insurance for the last 10 years, Marsh has actually put out a list of our top 12 controls to help businesses really prepare for the underwriting process. Joe, I know we might talk about it a little bit later on in today's chat, but effectively getting a firm understanding of these controls, things like multifactor authentication, employee training, vendor management, these are going to be key not only in the underwriting process, but truly whether you are a pizza shop or a billion dollar manufacturer, to be able to put some type of executive summary together on top of the

application to show to the underwriters that you're a little bit above the pack if you will. We've deployed certain technologies over the last 365 days, but what about for the next 365 days for the application period?

I would love to understand what your process or what the insurance process is, what they plan to do over the next policy period. That way that can be contemplated in the underwriting methodology if you will. It all goes back to really having a good risk profile. Now, how do you get a good risk profile? Starting with the top 12 controls is a great place. Making sure that you have somebody in-house, whether it be a CISO, CIO, or perhaps you have an MSSP, somebody outsourced that's really managing your cybersecurity. They're going to help you complete the applications to get started. Another area that we strongly recommend is when you're contemplating cyber insurance is looking at the panel, who's part of that carrier's panel. Now, from a legal perspective, a firm like Jackson Lewis is on many carrier panels. We want to make sure that your insured would basically have access to working with you, Joe, should they have some type of incident.

Same thing on incident response and credit monitoring and things like that. So making sure you know who you're allowed to work with and who's approved on the panel prior to the incident is absolutely critical. Thinking about claims, understanding the claims process, is this the first time the carrier's ever gone through a claim or is this their 10000th claim? Who are the providers that they're currently engaged with? Again, thinking about the panel. The rating of the insurance company, what is their financial stability? Are they going to be here next year to be able to pay out that claim? Are they admitted carrier versus a non-admitted carrier? These are all things that really need to be contemplated as you start to think about either buying insurance for the first time and or moving insurance carriers perhaps for a business that's been buying it for the past 10 or 15 years.

Joe Lazzarotti:

That's really great, really good thoughts. So there's a lot to consider, right? And it sounds like that having a seasoned, informed, qualified broker really will help through that process. Because there seems like some several steps that it's not just picking up the phone and saying, "Hey, I need cyber insurance," that there's a number of steps that an organization really needs to take as they approach that purchase.

Marc Schein:

Very much so, and perhaps today more so than ever, this is perhaps one of the most volatile markets that we've seen in the insurance industry. Thankfully it's now soft market rather than a hard market. What does that mean? There's more capacity in the marketplace, which is driving rates actually down. Just as Q2 2023, we actually saw about 4.4% of our policy holders receive a decrease. 18% of our policy holders actually increase their limits and why? Again, because there's more capacity in the marketplace than there has been perhaps over the last few years. So

Joe, we talk about mistakes or things that buyers may not necessarily be aware of. In real estate it's location, location, location. Perhaps price, price, price. Organizations that are so price driven often sometimes will sacrifice the coverage. Cyber policies are a little bit more customized than perhaps other lines of business because they have both first and third party coverage.

So you want to make sure when you're contemplating which cyber insurance policy to buy, is it going to provide coverage for things like wrongful collection of information, whether that be with the GDPR or BIPA, making sure that you don't have things like co-insurance and supplements within these policies. Subjectivities, we spoke about ransomware earlier on in today's chat. If organizations don't have multifactor authentication, they may get either no extortion coverage, ransomware coverage, or it may be dramatically sub limited. Perhaps there's ways to get these subjectivities in place prior at time of negotiation. Thinking about things like systemic risk, perhaps one of the most disturbing or challenging topics for underwriters today, really trying to get a handle of not necessarily one particular business going down, but perhaps an attack or a vulnerability or dependency that causes thousands of businesses to go down at the same time. And then we think certain industries may be impacted from cyber attacks uniquely. Things like healthcare, when we think about bodily injury and property damage arising from a healthcare incident could lose or cause some type of loss of life or loss of injury, things like that.

Joe Lazzarotti:

Okay. Yeah, and it's a good issue to raise because I think a lot of people worry, what kind of mistakes can we make? Kind of alluded to a couple. You mentioned first party and third party. Talk about that a little bit. Let's try to help, not everybody is going to understand I think those terms. So can you give the listener a little bit of understanding of what are the issues there?

Marc Schein:

So when we think about first party coverage, this is actually the dollars that we're going to have to spend in order to do the right thing. So in order to hire counsel to determine what our responsibilities are, what do state attorney generals we need to work with, who we need to notify, what regulators need to be engaged, that kind of thing. Hiring an incident response firm to figure out what happened, how did it happen, and getting those folks out, providing credit monitoring for the affected individuals, business disruption, things of that nature, all first party costs. If we don't notify and we stick our head in the ground and there's some type of lawsuit or we get some type of fine and penalty, that's going to be really covered under the third party, the liability section of the policy. And again, Cypress is one of those unique policies. Most are either first or third party. Cypress is one of the few that has both first and third party coverages incorporated into it.

Joe Lazzarotti:

Are there any other mistakes, Marc, that you think is important to raise? Just from what I see sometimes when we are not brokers, we do incident response, we do privacy litigation, we work a lot with carriers and brokers like yourself, and we also work with our clients before a breach

happens and after a breach happens. And some of the things we see are, I don't know if you're seeing this, how it impacts the procurement process, but companies oftentimes operate in silos and the people who may be in charge of risk management, they may approach something in terms of what they think, but they may not have necessarily a full picture of the whole organization and where those risks may materialize and then how those risks are treated for purposes of coverage. So that's just one thing that I see. But I'm curious maybe if you can speak to that and if that's something that you encounter, but any other mistakes that organizations should be trying to avoid?

Marc Schein:

So just to double click on that, we think about contractual limits, right? So oftentimes a company might say, "Hey, we just got a new contract and in order to satisfy this contract, we need to carry $1 million, $5 million, $10 million of insurance." Not necessarily linear to their risk, not necessarily have done any benchmarking analytics to determine that's too much insurance or not enough insurance. So really risk quantification would be one of the areas that I strongly recommend that businesses try and get a better handle on. Same thing, understanding Joe, I get a lot of times people say, "Hey, Marc, I have this under my bot policy, my business owner's policy, I have cyber liability coverage for."

And then we often look at it and it's maybe 10 or $25,000 of coverage. The coverage triggers are very narrow and they hang their hat on this coverage, and as we start to get a little bit granular and double click on that, they start to realize they either don't have the coverage that they thought they did or their coverage isn't going to respond the way that they originally contemplated or expected it would, and then they go buy a standalone cyber insurance policy.

So really relying on that throwing coverage I think is a major mistake for many businesses. And then also not necessarily taking advantage of all of the resources that you get from your cyber insurance carrier or broker. There's pre-breach services that are offered at no cost, being able to get on a phone with legal counsel or with an incident response firm to think about things from a proactive standpoint instead of from a reactive standpoint. Why the brokers and the carriers love this strategy, because if they're going to be able to engage you Joe, and they know that they want to engage Jackson Lewis in October and there's a matter that happens in January or February, well when that matter comes up, they don't need to start negotiating and interviewing with you and worrying about rates and statement of work and all that kind of stuff. This was all done prior to the incident and the carriers and the brokers love it because this helps reduce the business income loss that typically would arise or increase as more and more time goes by at time of loss.

I think one of the biggest mistakes is not necessarily thinking about how to respond prior to the incident and then really just waiting for it to happen and then responding retroactively, if that makes sense.

Joe Lazzarotti:

It makes a ton of sense. Seeing a lot of incident response planning going on, which is that's a positive development over the last couple of years. Speaking about a little bit of a historical perspective. You're going to know this much better than I, but maybe the last question here for us is, there's been quite a bit of development and transition in the insurance industry since the late 2018 or so until where we are today. There's been a soft market, some tightening and ups and downs. Maybe you can speak about that a little bit in the context of where we are today. You mentioned Marsh has some recommended controls. And so if I'm a business owner and I'm saying, "All right, this stuff is expensive, it's another bill I have to pay." What can I do given where the market has been and where it is today to be in the best position?

I know you mentioned thinking about working with your broker, coming up with a way to be in the best position for underwriting, but can you get into that a little bit more so that companies feel a little bit better about what next steps they should take?

Marc Schein:

So before we go into the proactive side, let's just take it back step into history. So looking at, call it 2015 to 2018, was the soft market for the cyber insurance world. Books were very profitable. Loss ratios were less than 50%. Oftentimes increases were flat or perhaps a decrease because you had so much supply outpacing the cost of demand. Once you got into 2019, 2020, you started to see claims pick up. Loss ratios were starting to near 100%. Insurers were starting to scrutinize the way that they were rating or their modeling. They really need to change their operating procedures. 2021, that's really where we saw the largest increase from a frequency and severity, the most notably around ransomware, so much so that you saw some carriers get out of the marketplace altogether. Other carriers that didn't started to increase their terms or their rates significantly.

Seeing 150 or 175% year-over-year increase in 2021 was not uncommon. Thankfully, in 2022, ransomware losses actually started to decrease in 2022. Combine that with an increase of additional premium and a change in the modeling that the carriers were typically utilizing and all of a sudden, 2022, we actually started to see rates start to come back down, and really the second half of 2022 is really when rates started to stabilize. When you're thinking about it from a rate perspective, as of Q2 2023, average rate increase is about 0.01% decrease. So again, you're talking pretty flat from a renewal standpoint. When we look at 2023 on a go forward basis, the market continues to soften, meaning that there's more capacity out there, meaning rates and prices are typically going down for organizations that can demonstrate that they are good risk and they have the good controls in place.

Now, Joe, you had mentioned some work that Marsh has done around underwriting methodology. Now, for everybody listening today's chat, they're going to have to fill out an application in 2023. They're going to then also need to fill out some additional supplemental

applications as well. Perhaps a carrier's concerned about a particular risk, they're going to want to double click and get a little bit more information on certain exposures. They should also be working on some type of benchmarking to determine what the right limit of insurance is, both from a confidential information, a privacy benchmark report. They should also be running a business interruption report to understand what would be the loss revenue should a cyber attack take our network down or we have some type of system failure. Lastly, a ransomware type of extortion type of report to model what other businesses perhaps either got from a demand standpoint, from the adversaries.

So in order to try and prepare yourself for that renewal. Marsh has also come out with our top 12 controls. And I won't go into any detail because I know that we're tight on time, but just for the listeners, so I think it's important for them to understand the top 12 controls. Multifactor authentication, that's number one with a star around it. If you don't have that, you're going to have a hard time getting ransomware coverage or extortion coverage in 2023. It's doable, but it becomes more difficult. Endpoint detection and response, making sure that you have secured and tested backups, making sure you have a PAM solution, privileged access management, making sure that there's email filtering and web security. Also, making sure that you have patch management and vulnerability management. Joe, I know something near and dear to your heart is making sure that you have a cyber incident response plan and making sure that it's actually being tested and on a frequent basis, making sure that the organization's doing cybersecurity testing and phishing awareness training.

Again, going back to the way that the adversaries are getting in, making sure that you have hardening techniques. Things like RDP are being closed down. Logging and monitoring protections, identifying your end of life systems, which has become a pretty hot topic as of late. And then also making sure that you understand who's connected to your network. Having some type of vendor or digital supply chain, understanding where that all comes out to be, and what I'd love to see an organization do is be able to provide a short summary on these 12 controls that we just discussed about all the great things that they've done previously, as well as what they're going to be doing over the next 12 months. That way, from an underwriting perspective, they have the application, they have the supplemental application, they have the benchmark report, and now they have what you're doing past and present and future around the top 12 controls. Going back to your first question, Joe, about a good submission or what makes a good risk profile, I believe those steps combined, that's what makes a good submission in 2023 and 2024.

Joe Lazzarotti:

That's terrific. Marc, this was really great. I really appreciate you taking the time. I think this information has been really helpful for our listeners in terms of understanding this is a process. You need to have good people around you to help you shepherd through that process and to be in the best position to secure coverage for what is really an important thing. I think our listeners have a lot to think about now and to take back to their teams as they evaluate their insurance

options as well as their preparedness. It's not if, but when. And a lot of people believe and address those cyber risks that are out there, it sounds like show. I don't see any signs of slowing. Marc, do you?

Marc Schein:

Unfortunately, no.

Joe Lazzarotti:

Well, listen, thanks again. This has been great. Appreciate everybody listening to our session here. Have a great day.

Alitia Faccone:

Thank you for joining us on We Get Work. Please tune into our next program where we will continue to tell you not only what's legal, but what is effective. We Get Work is available to stream and subscribe on Apple Podcasts, Google Podcasts, Libsyn, Pandora, SoundCloud, Spotify, Stitcher, and YouTube. For more information on today's topic, our presenters and other Jackson Lewis resources, visit jacksonlewis.com. As a reminder, this material is provided for informational purposes only. It is not intended to constitute legal advice, nor does it create a client lawyer relationship between Jackson Lewis and any recipient.