Risk Insights: Senior Living & LTC

Episode 19

Senior Living & LTC: Understanding the Impact of Third-Party Vendors in Cybersecurity

Welcome to the Risk Insights: Senior Living & LTC podcast, hosted by Tara Clayton with Marsh's Senior Living & Long-term Care Industry Practice. Each month, Tara, a former litigator and in-house attorney, speaks with industry experts about a variety of challenges and emerging risks facing the industry.

Tara Clayton:

Hello and welcome to Risk Insights: Senior Living and Long-Term Care. I'm your host, Tara Clayton. In today's episode, I'm joined by an industry expert to discuss certain cyber exposures in the senior living and long-term care space. For our discussion today, I'm joined by Sam Calmeyn, Vice President with the Marsh Cyber practice, US and Canada. Hey, Sam. Thanks for joining us today.

Sam Calmeyn:

Thanks for having me, Tara. I'm excited to be here.

Tara Clayton:

It should be an interesting discussion, but before we jump into, Sam, can you give our listeners just a little bit about your background and role here at Marsh?

Sam Calmeyn:

Yeah, absolutely. So I'm a placement specialist in the cyber practice at Marsh. I handle specifically cyber all day long, so it is my singular focus, throughout everything that I do. I work with clients ranging all industries primarily focused in clients that are a billion plus in revenue, but my portfolio has clients of- across all ranges of size.

Tara Clayton:

And I know, Sam, you work with a number of our senior living clients we'll discuss some of the specific real world examples that you've seen in- in helping our clients, but I think, too, what you bring to the table

is that experience you have really across industries. As we know, cyber is not unique to just one specific industry, so you bring a lot of value from that perspective.

Bringing this into the senior living long-term care space, I think similar to other industries we see a lot of partnering, reliance on third party providers when it comes to delivering care and services for our residents just really just making sure that our employees' n- needs are met, our associates and our residents, that, we're providing, we're doing our- our day-to-day type operations. And I have seen some different articles. I've talked with some different clients about, some of the exposures that they're starting to see from that third party vendor relationship in the cyberspace. And Sam, I know you've seen it really across it- various industries.

And that's really what I would like to talk about today, is this third party vendor and- and- and really what that can cause from a cyber situation starting there, what are some examples that you've seen from a cyber loss scenario when we're talking about vendor- third party vendor relationships?

Sam Calmeyn:

Absolutely, and there are two that I'll really focus in on and that would be the impact of potential data that you're sharing with third parties and then the actual business and impact if a third party vendor of yours were to have an incident that, prohibited you from continuing the operations as you normally would. The first is that impact on data. Oftentimes, organizations are sharing a wealth of information with third parties in order to just conduct their normal business operations. And oftentimes a lot of individuals think out of sight, out of mind. That data is with somebody else. That is not my responsibility. However, if the data was provided to you, you are still the custodian of that information. And if there's ultimately any breach that impacts that data, whether it happens at your organization or an organization that you're sharing that information with, you are potentially liable for the data.

And that can lead to potential third party liability claims We talked about some of these supply chain events that we've already heard over the course of the past year or two years. One that I'll point to that really highlights this potential impact to senior living clients is, uh, the moved event. A file transfer system had a vulnerability, where we saw a number of organizations impacted and it wasn't only those organizations' data impacted. It was some other vendors or the- their clients it would be the senior living center sending it to a vendor, but they had individuals impacted that weren't necessarily providing data directly to them. It was provided to their client and then that client provided it to another organization.

And that client that didn't even sustain the breach is still getting dragged into those lawsuits. The other large example, and, again, I'll point to another recent event just for, the sake of having an example, is the CrowdStrike event recently. We saw some really significant impacts across any and all organizations. And where organizations were unable to operate, that didn't only impact their business's ability to produce or generate revenue. It also potentially impacted their clients and we see significant business in our option losses quite frequently as a result of contingent business in our upstream, which would be that event occurring at one of your suppliers. So those would be the two largest ways in which we generally see that third party or vendor relationship impacting our insureds in ways that aren't covered until the scope of most cyber policies.

Tara Clayton:

I wanna dig in just a little bit on those two examples. One, the third party risk, the sharing of the data that you were talking about example. The claims that you all see, and- and the reason I'm- I'm kind of getting at this, is one of the- the topics that we've talked about quite a bit in the senior living space, not necessarily cyber, but in other type of arenas as it relates to claims is class actions. We see it with wage an hour, we see it on some of the resident sides, the staffing type class action claims. Is that something

that we see in the cyberspace as well as it relates to the loss of data through the loss- the loss scenarios you're describing?

Sam Calmeyn:

Absolutely. That's gonna be the most common way in which we see these actions brought against our clients, is going to be all of the individuals that were potentially impacted by this at signing up for a class action that is brought against both the organization who had the actual loss event where the data was impacted and our clients who the data was provided to.

Tara Clayton:

I like your point about I think a lot of times it's out of sight, out of mind. So I think these are really good things for providers to know, is just because you've passed it on to someone else, you don't delegate your authority and responsibility as it relates to the protection of that data. The second area is kind of big key loss scenario you were talking about was the the business interruption. One thing I kinda wanted to make sure to flag 'cause we've talked about this in some other episodes, actually I think just the last episode I- where I interviewed Mike Pokora talking about the impact of even if it's the third party that has the cyber event, what that can mean for a senior living provider.

And talking about business interruption, I know, Sam, we've talked about what you've seen in the- the broader maybe acute healthcare space as it relates to business interruption. Um, the inability to use equipment and really what that means, but, I think sometimes maybe senior living providers think that's not necessarily a big area for us because we're not using "technology" to perform operations and surgeries, but knowing that they are reliant for resident information, employee information - not having access to that data, what does that mean to you from a business standpoint? And if you lose that access, what do you need to have in place to be able to continue? Because we're 24 hours a day, right? We're at resident's homes. We don't stop working. We're there 24/7, so we have to be able to provide those care and services.

What about first party losses? Do you see that type of loss, uh, scenario in the senior living and long-term care space?

Sam Calmeyn:

Yeah, absolutely. I'll address the piece around business interruption first.

Essentially there's two components of a potential business interruption loss. There's an actual loss income that is incurred as a result of the incident, but there's also expenses that can be incurred in order to avoid potential loss of income or in order to continue operations as you would regardless of the event. And so those expenses can actually add up incredibly quickly. And as you've mentioned, senior living can get grouped into that broader healthcare space, but the risks are very different from a real, you know, emergency response hospital versus a senior care, facility. And where we see the business income loss being more impactful at those true emergency, services type risk, we often see extra expenses being much more impactful from the senior care living perspective.

And there can be a number of costs that you just don't realize that you have to find another workaround for if it is not readily available, uh, due to a cyber incident. I heard one example where there are- they were having to pay individuals to stand at doors in order to let people in, because their systems were down and they could not rely on their system in order to automatically open, close, lock doors. And so it's- it's even expenses that would never occur to you that you're gonna have to, incur as a result of these

events that still can be covered under these policies. In terms of first party losses, there is a wide array of coverages available under cyber policies, regarding these first party losses.

The most applicable example in almost every loss scenario is going to be breach response expenses. These can be expenses for legal counsel, if there was any type of impact to data. Connecting with a law firm to determine what are your responsibilities regarding that data that was impacted? Do you have to notify individuals? It could be the actual notification expense that can be covered under breach response. And then even if the impact was on your network bringing in computer forensic experts to determine. Hey, what happened? How did we- how do we remediate this event and how do we protect ourselves in court?

Tara Clayton:

Your example of where a provider had to, have this extra expense of having someone stand at the door to- to let someone in has me thinking. Okay, knowing these exposures, knowing that even though you're sending data somewhere else, you still have the obligation. You may have, requirements to notify individuals if there is cyber incident, just a whole host of things that have to be thought through. What should providers be doing now? Because I would imagine you don't wanna be in the heat of a cyber incident when all a sudden you start thinking about, "Okay, what do I need to have in place? Who do I need to talk to?" Right? What are some things that in your experience that you're seeing and maybe even talking with underwriters that they're expecting What are things that senior living providers should be doing now?

I hate to say it, but I feel like it's when an event happens at this point, not if an event happens, just because of how really dependent we are on, cyber related, connections. What tips do you have for providers?

Sam Calmeyn:

Absolutely. You hit the nail on the head when you said we should not be, uh, figuring out what to do at the time of a loss. there should be plans in place. There should be an instant response or a business continuity plan that we're looking to for guidance during the course of these events. And these plans should be tested on a regular basis. that is actually something that most cyber carriers if you have a policy in place with them, can either provide, depending on the premium level associated with the policy, potentially free or at a discounted rate, where they'll bring in legal, legal vendors to run through step by step a loss scenario with you. Day one, you notice your systems are down. some systems are potentially encrypted. What do you do? Go. And they walk you through from that moment 'til the ultimate resolution of the event. And having that exercise being completed prior to any incident occurring can be incredibly impactful on an organization's ability to respond to events in an effective and efficient manner.

And that's something that our underwriting partners are absolutely looking for, when doing application reviews, among the robust list of cybersecurity controls that they're also going to be requiring.

Tara Clayton:

I did an interview with one of our security consultants and his comment was around kind of these tabletop exercises, it sounds like, Sam, that you're describing that these cyber policies offer. The comment was you take action once you've actually lived the event kind of statement. I think that's a perfect example with the cyber because until you've really sat down and thought about how are all of our things connected.

If we're unable to access technology, what does that mean from our systems, from our door locks, from our WanderGuard systems, from, a whole host of different things that I don't think a lot of us appreciate how dependent and connected everything is until we don't have the ability to access that information.

Sam Calmeyn:

And doing- doing those events can even, help inform risk transferring for late and decisions as well because there are some really important topics that are gonna come up over the course of some of those scenarios that are played. One pretty applicable example to almost any insured is going to be the decision as to whether or not they would be willing to pay a ransom. Ransom demands have skyrocketed over the course of the past year, though we're seeing a decrease in the number of organizations willing to pay the demand, likely as a result of less and less insureds being willing to pay and more likely to restore from backup. So threat actors have to monetize, the access that they have when they have the ability to do so. And if you're going to be paying an extortion or open to the idea of paying an extortion, you potentially have a larger exposure as a result of those ransom advance significantly increasing over the course of that past year.

Tara Clayton:

I wanted to ask you, Sam, how can your cyber carrier or cyber policy, working with individuals like you, what else should, providers be looking at from that cyber carrier standpoint or looking at what their cyber policy can provide for them?

Sam Calmeyn:

There's a pretty, uh, large, variance in terms of the offerings that each carrier is going to be able to provide. one that comes to my head immediately in terms of having the more robust offerings in this space is going to be Beazley. . They have an entire cyber risk management offering suite of services that they're willing to provide to their insureds so knowing that and being able to take advantage of those services that are being offered is not only going to make your organization more secure and resilient a bit more, it also lowers Beazley's risk, right? (laughs) if- if you are more resilient. So it's really in the best interest of everybody that all organizations are taking advantage of these offerings.

Like I said, it's going to really depend on a carrier by carrier basis, what those offerings are for your specific organization, but it can be, potentially getting discounts on, cybersecurity solutions through vendors that these carriers have relationships with. It could be getting these tabletop exercises in place. It could be doing a review with your board in terms of what- what is our approach to cybersecurity? What do we need to be informed about moving forward? the list is really exhaustive in terms of what potential opportunities are out there to take advantage of.

Tara Clayton:

We're not just looking at price. We should be looking at what- what different offerings are there and how does that help support that individual provider's business plan, um, and goals as it relates to cyber exposure? one last question, Sam. I'm always impressed by our cyber specialist., knowing I used to be in-house and so I always, put myself in that position. And my first thought is always how do I get started even getting my arms around something like this?

And I know, again, you guys partner quite a bit with our clients and, Marsh has a, cyber scorecard, that I think's incredibly helpful, so if you could talk just a little bit about how we engage with clients I think to level set that first step of what is our exposure how do we take that next first step.

Sam Calmeyn:

Absolutely. There has, over the course of the past five years, been a barrier to entry for cyber. prior to the hard market that occurred 2020, we saw really significant difference in how carriers underwrote to cyber. It was really what's your industry, what's your revenue. they- maybe they'd ask you one to two questions related to security and then they'd provide you a quote and that was about it. And we saw that change essentially overnight in 2020 and now carriers are requiring these lengthy applications that are asking pretty detailed questions around, uh, cybersecurity. And that isn't always the easiest application for some of our partners to fill out and so that is something that, you should be consulting your broker about. And how can they make it easier on you, in terms of, completing this information gathering process?

because there will be a substantial need for information as you go through the process of trying to procure a quote, as each carrier is looking for different pieces of information around security that they deem valuable in terms of measuring your risk.

Tara Clayton:

Thanks, Sam. To me, the big takeaways that I heard today from you are, we're in an environment where everyone needs to be prepared for a cyber type event to happen and understanding what your exposures are and how it will impact you either through third party loss, first party loss, or even the business interruption with the extra expenses. That we know that's a big area for our clients on the extra expense part of it because, again, we are open 24/7. So Sam, I really appreciate you joining us today and really high level I think opening everyone's eyes to things they need to be talking about with their broker and their cyber specialist. So again, thank you for joining us today.

Sam Calmeyn:

Thank you for having me. This was a great conversation and, uh, really appreciate the opportunity.

Tara Clayton:

For our listeners, you can learn more about third party vendor risk in the recently released Marsh cyber thought leadership entitled Third Party Cyber Risks Impact All Organizations, which will be linked in our show notes.

Be sure you're subscribed so you don't miss any future episodes. And as always, thank you for tuning in, and I hope you'll join us for our next risk insight.