Cyber Risks – How to Help Prepare Your Institution

Cybersecurity continues to be a major concern for most independent schools. This **on-demand** webinar reviews the current landscape of cybersecurity breaches, address security protocols that can be implemented, and provide guidelines to help you enhance cyber hygiene practices. This session also provides guidance on cyber insurance and the various issues independent schools need to consider during the application process.

Find additional resources on our event page: https://claconnect.com/en/events/2022/cyber-risks-how-to-prepare-your-institution.com

Here is a transcription of this session:

John Toscano:

Hello, and good morning everyone. On behalf of CliftonLarsonAllen and Cross Insurance, welcome to Cyber Risks, How to Best Prepare Your Institution. I'm John Toscano and I'm CLM with CLA's Connecticut office from which I lead the firm's independent school industry practice. Our objectives during our time together this morning will include a few things, which we'll see on the slides in a few minutes. So walk through the current cybersecurity landscape, an update on cyber attacks, including some of the top causes of today's data breaches, and then my colleagues will lead a round table discussion where we can share our experiences and other insights. We'll also make sure to leave some time at the end of the session for questions and address any other thoughts folks may have. So without further ado, I'm going to pass the mic over to my fellow CLA principal, Jeff Ziplow. Jeff, take it away.

Jeffrey Ziplow:

Thank you very much, John. Glad everyone could be with us today. And I think, as John was mentioning, cybersecurity is an extremely important topic for discussion. And what I thought we could do today is just do some level setting and talk a little bit about what the current cybersecurity landscape is and looks like and spend most of our time, however, in a round table discussion. We've got two very talented people online with us. David Nowacki, who's a director at CLA in cybersecurity. He has 18 plus years of experience. We also have Amy Reese, who is with the Cross Insurance Agency. She has over 15 years of experience as a management liability and cyber underwriter, and she handles many of the Agency's, Cross Agency's, largest and most complex cyber accounts. And I thought that bringing together this team of people would be a great opportunity to learn more about not just the theoretical, but most importantly the practical elements that we need to start thinking about.

So what I'd like to do is share a little bit with you about facts and statistics of what we're seeing. So as you can see on the screen, every 39 seconds, there's some type of hacker attack. We have recognized and seen a significant increase since COVID in what those attacks are, how the attackers are trying to get into our systems. But one of the things that has become very apparent is that, and you can see it on the screen, 95% of the cybersecurity breaches are facilitated by human error, typically, phishing, typically phishing, but 95% are by human error. And that's an important statistic and we'll get into more of the details behind that in just a little bit.

We've heard a lot about this thing called multifactor authentication. When you're logging into accounts, only 50% of organizations require, or 50% of the organizations don't require multifactor authentications.

So that's an interesting statistic for me because multifactor is one of those things that can really save an organization from a significant breach. And again, more to come on that. Ransomware. We can't spend an hour a day a week without listening about some type of new ransomware. It is certainly on the rise. We're seeing that it's estimated it costs 600 trillion annually and it's going up exponentially. So ransomware is something we need to be thinking about. And you can see the other items here. It's really important to think about cyber insurance. Only 55% of organizations claim to have cybersecurity insurance. Is that true? Is that not? Well, I think we're going to hear more from Amy Reese about that and get her perspective.

One of the things that has certainly gotten me to think a little bit is the average amount of time that an attacker is in our systems or has when a breach is recognized. And if you look at the statistic here, on average 280 days before someone, or 207 days before someone identifies that a breach is going on, 73 days to contain the attack. So what we're learning or what we have learned is that people are coming into our networks, they're finding ways of getting compromising credentials, and they're in our networks for, in this case, 207 days looking around, trying to identify where those crown jewels are, where key information is that they can take out and exfiltrate. And then we get into those incidents where we have to think about ransomware as well.

The cost of a data breach, not insignificant. As you can see here, it depends on the number of records that are exfiltrated, but if we're using that 79,000 as a number, it basically costs 2.8 million or more to deal with that breach. Some are a little bit more, some are a little bit less, but it just gives you an idea that this is a very costly situation. If you do have a data breach, it's really important to minimize the cost. More importantly, let's proactively figure out ways where we can mitigate the risk of a data breach.

The importance of cyber insurance. Cyber insurance has changed significantly over the past several years. It's not a nice to have anymore. I would tell you it's a need to have. I think we're going to learn more about what are the considerations of cyber insurance and why do independent schools need to be thinking about cyber insurance and protecting their environment. We're going to be getting into what does cyber insurance cover. You can see here, covers the cost of response and damages. Does it cover other costs that we need to be thinking about?

So let's just take a quick review of what those cyber attacks are looking like today. A lot of the data breaches are starting out with stealing of passwords because it's much easier to steal passwords, someone's credentials. And once we get those credentials, we can then get into the various systems, look around and identify where those crown jewels that I mentioned are. Phishing. Phishing remains to be one of the top attack vectors. I think you've probably received all of those on the webinar. You probably receive some type of phishing, if not on a daily basis, certainly on a weekly basis. This is certainly an example of one type of phishing, but there are many others as you can imagine.

One of the things that we are seeing is that by those credentials being compromised, most of the time the activity is financially motivated, that they're going to be some type of ransom. There's going to be some type of call for monies to be paid to the attackers in some way, shape or form. Ransomware I mentioned earlier, it has evolved. It has changed over the past few years. As companies did a better job of backing up their systems, ransomware evolved and it's becoming a concept of double extortion. Before the data is being encrypted, as I mentioned earlier, people are in your system, they're looking around, they will exfiltrate out information and put it on the deep dark web. And if you don't pay them the ransom, they're going to release that information on the deep dark web. And that's that sense of double extortion.

There's a new model out there, I don't like to call it a triple extortion, but the triple extortion is if it doesn't seem by the attackers that you're going to be paying, they're going to reach out and start calling clients to put pressure on you to pay so that the client's information is never released.

And then lastly, we can't forget about the CEO fraud situations regarding wire funds. This is through phishing attacks. We're seeing more and more situations where people are getting attacked, phished, spear phishing and asking to pay for various types of money cards. I've seen situations where Apple iTune cards or Apple cards are being requested and we just need to stay on top of it. We need to understand the reasons why. So with that, what I'd like to do is spend our time in a round table discussion. Again, David Nowacki, Amy Reese, they've got tremendous experience with cybersecurity, extremely knowledgeable. And so what I'd like to do, David and Amy, is very first question, and David, why don't you start us off. Why are independent schools being targeted for cyber attacks?

David Nowacki:

Yeah, thanks Jeff. I think one of the primary reasons, and I will say the trend is not going away anytime soon, is the evolution of these ransomware attacks, they started out by targeting individuals and businesses where there's a larger pot of money. And over time those organizations increase their security posture, whether it's through realizing that there's some monetary exposure or regulation dictates the level of preparedness be increased significantly. And so what we're seeing from a trend perspective is the opportunity to move into sectors like independent schools is greater because of the lack of opportunity in others. Doesn't mean that targeting larger organizations, more highly regulated industries is going away, it's just that they're moving into smaller businesses, they're moving into education because they aren't, in many instances, as well funded. They don't traditionally have the same level of budgets for IT or for end user education awareness. Some of these other things that we've seen trending upward in a lot of other industries for years.

And so, one of the primary reasons is that's where the bad guys are looking now, and it's going to continue to rise and evolve over time. Another reason, another why, and there's probably numerous whys, is just student information and financial information that may be in locations that are easier to identify, maybe not as geographically disperse. And so, an independent school is generally single campus, smaller organization than a bank or a credit union that has 35 different locations. And so targeting them becomes a little bit easier as well, knowing where the sensitive information may reside, as well as knowing how to attack and where to attack from. And so those are two of the bigger trends that I see as to why independent schools are being targeted for cyber attacks.

Jeffrey Ziplow:

Amy, any thoughts on that?

Amy Reese:

Yeah, so I would echo what David just said about the security and the safety of both the students and the staff, as well as the privacy of both personal and healthcare information being important. And then specific to this group, I would say that also donor information is important. So if you have alumni that are donating to the schools, definitely an exposure to think about.

Jeffrey Ziplow:

Do you see increased risk associated with that donor information?

Amy Reese:

Absolutely. Especially if you've got celebrity status donors or high net worth individuals, there's certainly more scrutiny on protecting that information, especially if the dollar amount was ever to be divulged. So for sure, on this call, I think that probably resonates with a lot of the schools.

Jeffrey Ziplow:

Sounds good. Amy, I'm going to start with you on our next question. What are the most common breach scenarios you see for independent schools? Any thoughts on that?

Amy Reese:

Most common, I would say if you're using a system like Blackboard where you have students that are doing instructional classroom activities and it's hosted online, or they're putting their thesis for their senior year into that kind of program, you have students who are applying to pretty prestigious colleges in the future, so protecting that information is important. And so I think that the hackers are looking for ways to scare the schools. Like David said, typically you see that schools don't have as much money to put into an IT budget as other businesses, but I think the last 18 to 24 months, we've seen a big improvement in controls across the United States with every class of business. So that has certainly helped.

I'm trying to think of another claim I've seen recently. I would say dependent business interruption with, if you are using an online system to have tuition paid, the hackers will go after that because it's the easiest way to access money. Probably a lot of the folks on this call have something like that in place where they're relying on a vendor in order to have either donations or tuition payments coming in and the loss of business income and operating expenses you would experience from that. So there's something in the cyber policy called dependent business interruption. It's one of the insuring agreements, and that's where I would see a lot of claims coming into for education specifically.

Jeffrey Ziplow:

Got it. David, any thoughts?

David Nowacki:

Yeah, plenty of thoughts. So I think in some of these scenarios are very similar to other education organizations, whether it's higher ed or K-12, but there's probably three or four different scenarios that we are seeing trend upward. One is a targeted attack, and Jeff mentioned earlier, CEO fraud or wire fraud. It's also called business email compromise. So if you are publicizing, if your private school is publicizing some type of capital investment that involves building a new building or soliciting donations to expand educational program or something like that, the bad guys know that. They're going to directly target your organization and they may mimic the organization you've hired, the construction company you've hired to build a new building, expand campus. They will spend months trying to socially engineer their way in and then develop a relationship with your persons and your accounts payable department or controller and try to coerce you into sending money to the wrong location.

Very simple scheme, but they invest months in the relationship, months in socially engineering your persons into doing that. It's not a typical cyber attack, but it is an attack that you need to be aware of. The direct access to cloud accessible systems, so whether it's your donor management system or something else, sometimes it's a pain to require things like multifactor authentication. Certainly, we'll talk about that later on as well as a control improvement area, but you don't always want to inconvenience your donors. So they'll do a direct attack on that cloud system, try to capture credentials, try to harvest financial information in scale, and then sell it on the secondary black market. So that's one of the areas among the scarier ones. And Jeff mentioned earlier about the trend of having 200 days in your system. That doesn't necessarily mean your system that's providing access to your faculty and students.

That could mean a cloud system as well, could mean your email system. So if an organization successfully phishes one of your employees and you're using Microsoft 365 for email, for example, once they take over a user's inbox, they have that person's identity. They can move two different directions when that happens. And imagine someone in your donor department who's managing those relationships starts to socially engineer your donors to sending information to a different system, to a different bank to directly wire money outward, and impersonating you for 200 days. What's the impact there? When would you realize the attack has occurred, and what's the financial impact? And does that covered traditional things like cyber insurance? These scenarios are highly sophisticated and we're seeing not only the direct access to records and systems trying to cause business disruptions, but stealing identities and owning identities for months at a time.

And these types of schemes aren't being counted in the same way as a typical ransomware attack or a breach attack because it's categorized as a multi-prong approach. You have the compromise of a system, you have social engineering, and you have individual incidents that attract over time. Those are scary as heck, in my opinion, to see something like that.

Jeffrey Ziplow:

Both David and Amy, one of the things I'd just like to add is, and in doing some of the work that we do, this is with David actually, is that there are times where people will put in new systems. And the one that happened fairly recently was they were putting in a new physical security system, the cameras, the door locking, the electronic type of surveillance capabilities and great system. The only problem is that the third party vendor that implemented the system, left the default credentials in the system. And so anyone could essentially go out and access the system outside or through the internet, and using the default credentials, which is very much available online through just some very quick Google searches, could actually open doors, lock doors, and/or move cameras around. And so those are things that we really need to be thinking about along with these additional systems that we don't think about as part of our network, but the voice over our phone systems that are typically connected up, or the HVAC systems that are typically connected up. We certainly have seen some breaches through those areas.

Amy Reese:

That's a great point, Jeff. Just want to touch on that. When we talk about the safety of the students and the faculty, that's spot on with the technology that we see now with security measures. It doesn't just include the internet, but it includes the physical security controls and the escape route. If you have a hostage situation type plan, we've seen those being exposed. We've had a client that the hackers locked down their warehouse and turned up the heat to 100 degrees, basically trapping the employees in there, ruining their product because they're able to control the heat too. So, good point.

Jeffrey Ziplow:

Hey David, quick question. A question came up, are you seeing any prevalence in fraudsters obtaining a bogus email address or mimicking a domain or email address of similar users? What are your thoughts?

David Nowacki:

Yeah, if I understand the question correctly, whether they directly compromise your email or they register a new domain that spoof shores. So that's one of the most common attacks, especially in a mass scale... sorry, in a targeted fishing scheme. So your organization may have an I in it and they change it to an explanation point, but everything else seems the same. They'll register that as a new domain, it will be trusted, if that makes sense. They'll launch a campaign that will get through your basic email and

spam filtering measures. Most current generation email systems have an ability to filter out malicious, know malicious domains that are likely to be launching attacks. The targeted attack scenario is they'll either compromise your system and then launch outward, or they will spoof your system and then coerce you, make it look like you are receiving an email from someone in your organization and then target individuals and target business lines to try to get them to respond to click, to download, to enter credentials or the like. And so yes, that's one of the most prevalent attack methods out there.

Jeffrey Ziplow:

Got it. So we talked about people as people being compromised and I'm very interested in your thoughts, Amy, your thoughts on who do we need to be more concerned about? Is it teachers, is it school administrators, is it students, is it other vendors? What are your thoughts on that, Amy?

Amy Reese:

Yeah, so I think based on the vast marketplace of cyber carriers that we work with, students are absolutely where the underwriters are most focused on. I like to call this peopleware, where you can have all the right IT controls in place, but you're only as good as your people. And if you have faculty, staff, students clicking on links and emails, there's your exposure too. So most of the carriers do want to see phishing training performed at least quarterly now. It used to be annual, then it was semi-annual. Now it's quarterly because you just keep having to remind everybody that this is just so common. And piggybacking on what David just talked about, I like to use claims examples because we can talk about what's in the form, but I think it resonates with clients more when they hear the real life claim examples.

So we have a very large client who has 25 plus people on their finance team, and they got an email from one of their "vendors." So the email was spoofed, it wasn't our client's breach, the vendor was breached, and the vendor emailed our client saying, "We changed our banking information. Please pay the receipts going forward to this Bank of America account." So now this client has protocols in place to have three people review any banking changes before payment is sent out. So they had three people, including their senior vice president of finance sign off on this. And what do you know, it was a fake email account, fake or fraudulent bank account, and they transferred over $700,000 to this fake account for four plus months. And then the vendor says to them, "Why haven't we been paid for our product in the last few months?"

So that's where that came from. But the message is this client had protocols in place to prevent this from happening and none of their people followed the protocols, including the most senior person on the team. So as a cyber risk manager, I will implore you, make sure you have those policies in place and make sure part of it includes calling the vendor to confirm that change before you start making those payments.

Jeffrey Ziplow:

This happens all the time, doesn't it, Amy?

Amy Reese:

Absolutely. It's scary. And many years ago I was a crime underwriter before social engineering became part of the cyber insurance. And we used to call this the dummy clause, where if someone calls you up and says, transfer me a million dollars, and you do, you're a dummy. But now the hackers have become so sophisticated in how they trick you that that was how the social engineering endorsement came about.

Jeffrey Ziplow:

David, do you have a difference of opinion as to who we need to be more concerned about or anything to add there?

David Nowacki:

Not different, just complimentary, which I would say it's everyone and it depends on what risk you're looking at managing. And each one of those bullets right there, and the other, I'll expand upon in a second, but they are a source of social mining information. So I'm just trying to get snippets so I can use it, especially in a targeted attack scenario, you're trying to get a little bit of information out of a department head, out of a teacher, out of an educator, so you can use that in the next stop on your social engineering tree when you're trying to get into an organization. And this concept of reinforcing your awareness protocols and controls across every bridge of your organization is absolutely paramount. This practice area I call patching your people. So you're familiar with patching systems, operating systems, supplying windows updates. This is patching your people where you have known gaps and making that a routine maintenance activity to make sure they're aware.

It takes one clicker for an organization, a clicker combined with some type of a misconfiguration to allow a foothold in your organization. Once they have a foothold, it really depends upon how robust the rest of your controls are, your detective measure is, how aware you are of the indicators of compromise, et cetera. So we see this happen all the time when we do assessments proactively, where we're hired to do phishing expeditions, social engineering expeditions, penetration tests or vulnerability assessments of private schools and other organizations where we send... They're educated, they're doing phishing and they're doing traditional training as well. We send 200 emails to the administrators plus faculty and one person clicks, they also happen to enter their credentials and then I have an ability to log in remotely because of a misconfiguration in multifactor authentication or something else. And so it is very, very concerning.

That other bucket I think we're going to continue to talk about. But I think the other involves IT staff. It involves, for smaller private schools, the competency of your managed IT providers if you're outsourcing some of the management of IT. And so they have a high level of responsibility for some of these organizations and in some case it's blind reliance instead of educated vetting of what they're doing on the security front or paying a little bit more to make sure that they're going the extra mile, so to speak, to help you secure your systems. And so it's everyone, but it's also depending on the risk.

Jeffrey Ziplow:

Great, thank you. I think what I'd like to do is, we've been talking a lot about cyber attacks, but I think equally important or even more important is how do independent schools need to prepare for potential cyber attacks? And I put some bullet points down here, MFA, multifactor authentication, backup training, incident response, you can see the list. David, your thoughts on what are your top three, top five things that you need to be thinking about or should the independent schools be thinking about to prepare for a potential cyber attack?

David Nowacki:

Yeah. I wouldn't order them in any particular order. I would say you need to have a layered approach to security and looking at ransomware and email phishing as the most likely attack scenario. The next would be some form of business email compromise, compromising a wire transfer, ACH or funds in some way. So those two.

Jeffrey Ziplow:

David, I want to go back to your comment about layered. Give me a definition or better explain what layered means.

David Nowacki:

Oh, right. So layer number one is making sure that... And it's layer number one and layer number 10 depending on how you look at it. But typically you think external perimeter of your network. So firewall, making sure the bad guys don't get in and authorizing only trusted traffic, that's a traditional layer one. And then layer two, assuming they're in, and I'll talk about from a network and a people perspective, layer number two would be how are you segmenting? How are you sectioning off your network? Is it all one network? Once I get in one layer, if the firewall's compromised, can I see everything? And what levels of access controls do you have in place? Layer number two. So if you're separating those out or requiring separate logins for each system, you have more layers of security there.

There's physical layers as well. So geographically separating the location of systems, locations of people, the locations of data. So that's where the concept of having an offline backup comes into play, having reliable disaster recovery, business continuity solutions, whether it's an ability to replicate your systems and fail over, et cetera. So you have more layers there. Layers of people are some of the controls that we were talking about previously on having three levels of approval for a major transaction. So there's layered security, there's separation of duties, it's also coined like defense in depth. So that's the concept of layered security. Is not just having one-stop shop for everything or one control fails and you can't detect it, you can't prevent the propagation of an attack and everything. It goes out the door if one control layer fails. So that's the concept I was talking about there.

Jeffrey Ziplow:

Thank you. Amy... Oh, I'm sorry. More, David?

David Nowacki:

Let Amy talk.

Jeffrey Ziplow:

I can see David, you're a bit passionate about this.

David Nowacki:

Right. Right.

Jeffrey Ziplow:

Go ahead Amy, your thoughts. What do we need to prepare for?

Amy Reese:

I guess what I would add there is basically I think of it from the underwriting side and what has changed in the past year with requirements. And MFA, we've all heard about a million times, we're probably all sick of hearing about it, but MFA has been put in place for the most part by most businesses now in the United States. So the hackers have to come up with different ways to get in. Firewall, I would say password management, having a password management tool, if you have any administrative right accounts, having very, very strong password management controls for those, is important.

I've seen a claim where an employee gave a friend of theirs access to their team's account because they were retiring and wanted to transfer some of their personal data onto their computer at home. So having protocols in place to prevent employees from being able to share those credentials is something that we've seen arise with the carriers wanting to see. And then segregated air gap backups being another hot topic now, because the thought process is if you have a ransomware attack and the hackers hold your data, but you have it elsewhere, stored somewhere else, you can say, "Go ahead and take my data. I have it somewhere else. It doesn't need to be recreated now." And so, they have less hold over you now at that point because the data is elsewhere.

Jeffrey Ziplow:

Amy, you used the term air gap, you want to explain that?

Amy Reese:

Oh, I'm probably not the best to explain it. I'm not an IT expert. But having it stored separately, a lot of times they want to see a physical copy more so than having it in two different cloud scenarios because we're all relying on the cloud for our data for the most part, at least in one place.

Jeffrey Ziplow:

Got it. On this list, and I think we've talked about a bunch of them, and we'll get into cyber insurance in a bit, but incident response, is that something that an independent school needs? Is that a nice to have? Is that a have to have? David, your thoughts?

David Nowacki:

Yeah, and I would say along with the cyber education awareness and training component is the most important process related control. And it doesn't mean that you have to deploy systems, although in an ideal state you'd have. You'd have security systems that would aggregate logs and alerts and look at where a threat may have originated, what happened, et cetera. All of that data from a forensic reinvestigation perspective. You may not have the benefit of having that. But incident response, incident handling, triage, escalation, and that communication component are critical. And knowing how quickly you can identify a potential incident, track it as an actual potential incident, not just assume that it's a one off scenario, and then communicate internally so that you can mobilize your internal people, third parties, call your cyber provider to see if there's a cyber breach response service that you can tap into early on. So you can start to preserve that evidence. If it's associated with the business disruption, you can start to preserve the evidence, do the forensic investigation, all the scoping while returning to normal operations.

So those two tiers, the quicker you can get to this is something we need to move on, the better. So it's absolutely critical to be working on how you do that from a process communication perspective.

Jeffrey Ziplow:

I guess I would also add, David, that you don't want to be thinking about how you're going to perform an incident response during a crisis situation. We tend to make bad decisions, right?

David Nowacki:

And so doing things as simple as simulations or tabletop exercises, they may feel like they're check the box type scenarios, but if you challenge yourself and ask questions or have someone who's a facilitator

come in and help you, you're going to have a bunch of unknowns and that's where there's opportunity to improve in terms of that. And I do have some other comments on that other bullet if we have a minute as well.

Jeffrey Ziplow:

Go ahead.

David Nowacki:

So MFA, we talked about that a little bit. I would say start with anything that's accessible externally to the organization. So cloud systems that aren't inside the boundaries of your firewall, your physical infrastructure. Next level is anything that has privilege, high level privilege, whether it's administrative account or other, no brainer, MFA. And then work all the way down to users as long as that's not overly burdensome for the operation of your business. Hardening those systems as well. So the concept of patching systems, we need to have security systems deployed first with security in mind. So making sure that you're hardening your cloud accessible systems, making sure you're patching systems, making sure you're identifying vulnerabilities, doing vulnerability scanning, and then remediating known exposures in a timely fashion as well.

Jeffrey Ziplow:

All right. I want to spend some time on cyber insurance. And Amy, I've got a couple of questions for you that you have that expertise that we're looking for. First and foremost, why should independent schools have cyber insurance? And that is assuming you believe that they should have cyber insurance.

Amy Reese:

Yeah, that will be correct. Maybe I'll start with following what David just talked about with the incident response plan. Part of it should be sure engaging your carrier as soon as you're aware of an incident. And one thing I'll recommend there is assuming you have cyber insurance, having the claim information ready to go, so who to report the claim to, your insurance agent's information, keeping that as a paper copy, I would recommend. Because what happens is you get breached and your network is shut down, you can't access your email or anything else, and then you go and you're like, my cyber policies online, how do I find who to report this incident to? So keeping it separate and printed out, I would always recommend. But sure, we have clients who will say, "Look, we have really strong IT controls in place. We've spent $50,000 this year implementing MFA and backups and EDR."

So there is sometimes hesitancy to purchase cyber insurance. But what I would say about that is do your IT people know how to notify everyone whose information is breached because every state has different privacy laws that you have to follow and abide by. So the notification part I think is huge. And then two, if you have on staff IT or you're outsourcing it to a vendor that you're paying and there is an incident, do you want those people defending their own advice in a breach situation? So having a carrier who has their own vendors that will do the forensic research and legal, I think is one of the benefits of cyber.

And then the third thing I'll talk about and that this is a lot of what I'm seeing now in the marketplace is the dependent business interruption where hackers are trying to go after businesses that would cause a widespread event. So if we're all using Microsoft, how many people would that affect? So that's a big one to, where I've talked about if you're relying on a third party vendor to accept donor payments and tuition payments, you can only control so much. So you can have all the right IT controls in place, but if your vendor is breached, then the policy typically has coverage for business interruption that you

experience from not being able to accept tuition payments and you're still having to pay your faculty and staff. So that's one of the nice benefits of having a good cyber policy.

Jeffrey Ziplow:

Thank you. Just because of time, I'm going to jump into the next question, which I think is really important to understand. What are the underwriters looking for when they're evaluating independent schools in cyber application? And I just put some bullet points there, I'm not even sure they make sense. Amy, what are your thoughts?

Amy Reese:

Yeah, like I said, the phishing training, because there's a huge concern about the student behavior with what they're clicking on is a big one. So there's typically an application question that says, "Do you perform phishing training at least annually?" So sometimes now we're seeing follow up questions where they want to ask, okay, that's great, you do it at least annually, but how often are you actually doing it?

Jeffrey Ziplow:

And do they ask questions? Are you using a third party vendor for it or are you doing it internally? Do we need to be concerned about that?

Amy Reese:

I would say the vast majority of businesses are using a third party vendor. KnowBe4 is probably one of the most common ones. And just something for everyone to know that's on this call, if you're using KnowBe4, there are some carriers that will offer you a discount on your subscription as a policy holder. So I would look into that. Beazley, for example, is one of the carriers that does offer that discount and they are one of the largest writers of cyber for schools. So something positive to note there.

Jeffrey Ziplow:

Thank you. Yep. Great. What about these other items? Are the underwriters concerned about backup? Do they care about written policies and procedures? Do they concern themselves about where the crown jewels or the information assets are? Is that important to them or no?

Amy Reese:

Yeah, all of the above. Years ago, cyber used to be just based mostly on the class of business and revenues, but now it's become more the, if you don't have these controls in place, you can't get the coverage. So unfortunately it is all of the above with having controls across the board.

Jeffrey Ziplow:

And Amy, what's one of the biggest changes that you've seen in this past year as related to underwriters looking at these types of cyber insurance applications?

Amy Reese:

It really pivoted from MFA to backups. So backups and then a lot of questionnaires on how much reliance you have on vendors. So again, the dependent business interruption with how it would cause a widespread event. And what I'm starting to see now that I think will be very significant for 2023 is the carriers pairing down on the widespread event catastrophic exposure, where they're going to look at

cutting the limit for ransomware events or the dependent business interruption and sharing agreement if there has been an outage for a certain period of time. So we've seen one so far that was six hours long that one of the vendors was out that caused a wise part event. I think the policies will have a much broader range, hour-wise, that will be so concerning, but I'm starting to see that.

Jeffrey Ziplow:

Great, thank you. I'm going to move on to our next question. And David, your thoughts on what do we need to be thinking about when we use software as a service or third party vendors? I provided some thoughts here about different types of services, payroll, credit cards, but really cloud vendors or manage service providers, what should we be thinking about?

David Nowacki:

Yeah, so the first thing that I would say is everything on the last two slides. First you start there. So you're asking them about MFA, backup, inventory, where data is, all of that needs to be asked up front, don't assume. So you don't assume. I'll start there. The next level is probably two or three different tiers. One, do they have an independent assessment of their security controls? So think SOC one, Service Organization Controls 1, or SOC 2, or some type of independent assessment that says they have a strong security posture. There are ISO security standards, International Standards Organization. There's NIST based standards. There's federal standards for assessments. So has this cloud environment been assessed and can they produce a report that says the controls are sound? That's the next level.

And then the third thing to really think about is where? So is it in our geographic borders? So many SaaS providers are using data centers that may be in other industries, other countries. Are you okay with that? Are you not? Do you need to pay a little bit more to assure that it's geographically located in the US only? Because whether it was Microsoft, Azure, AWS, or any other SaaS provider that's using those platforms or other platforms, you need to ask those questions. And then the last one is encryption. Don't assume that they're using sound encryption practices, and we didn't talk about that on the previous slides, but is it encrypted in transit? Is it encrypted at rest? Are backups that they're using encrypted? The whole concept of encryption needs to be asked in multiple levels when it comes to SaaS providers because it's not under your four walls, so to speak. So you need to make sure that it has that logical level of encryption as well.

Jeffrey Ziplow:

Great. Amy, your thoughts on third party vendors?

Amy Reese:

Yeah, it's become such a hot topic right now with everyone's relying on an MSP or some kind of software provider for everything. And by utilizing a third party vendor, you are further exposing your data, your customer data, your donor data by having to rely on a third party. So it's just the claims that we're seeing coming from that now are just, I think, like I've said, the new wave of the cyber insurance concerns.

Jeffrey Ziplow:

So let me ask you a question, and I know maybe a tough question to answer, but I'm an independent school, I have cyber insurance, I'm using a third party vendor for payroll or donations, doesn't really matter, they get breached. Am I covered being the independent school through my cyber insurance policy?

Amy Reese:

That is a great question, and I get that question at least once a week, because a lot of times we get pushback on do I need cyber insurance because we use an MSP or we outsource? All of our data is stored in the cloud. We don't host it. And yes, you are the point of sale, so you are going to be pulled into the claim. And sometimes it's just a matter of utilizing your cyber insurance to trigger the forensics part of the policy to figure out how the breach occurred, whose data was breached? You could have five people on staff whose data was breached in a breach that was primarily from that vendor who they had 10,000 people's info breached. So you're still going to have to defend yourselves in a situation on the liability side. But yes, your policy is designed, assuming it's a standard market policy, to protect you because you are sharing data with third parties and there's not many businesses who aren't sharing some sort of data with a vendor.

Jeffrey Ziplow:

Got it. Thank you. David, anything else? You good?

David Nowacki:

I'm good.

Jeffrey Ziplow:

Okay. We're going to move on to our next question, which I'm very intrigued by how you're going to respond. So what are your 2023 cyber predictions? David, what are your thoughts?

David Nowacki:

I was going to save it for this slide because it's on the previous slide, but everyone is going to be so annoyed with what they have to do to manage supply chain risk and third party risk management. I think the emphasis is going to be on how you're managing it, how knowledgeable you are. It's the opportunity where... For the mass event, so we saw last year in the solar winds breach incident that impacted multiple industries and organizations, how are you assessing the risk? How are you evaluating the resiliency of your business operations as it pertains to single dependence on vendors? How are vendors, especially software as a service providers, able to answer the question about what are the components of their system, the fourth party risk that may be susceptible to vulnerabilities? And so I think it's going to be, and my prediction is you're going to be annoyed with how much emphasis is on this, but it is the next emerging thing that won't go away, is third and fourth party risk and supply chain risk management as it pertains to cyber.

Jeffrey Ziplow:

Amy, your thoughts?

Amy Reese:

Yeah, absolutely. I'm a broken record now on the contingent business interruption situation, where we're starting to see the questionnaires about how reliant you are on third parties in order to operate on a daily basis. And again, that's where the hackers are starting to focus their efforts on, because they can go after one risk and get 300 grand in a ransomware payment, or they can go after somebody that would potentially affect hundreds of thousands of businesses. And those are the risks that are more likely to pay out huge ransom payments.

So that's absolutely where I see the cyber market going. The good news is, I do think, and hopefully no one's recording me on this, I think that the premium is starting to level off. I think in the last 18 to 24 months, the schools in particular got hit really hard with premium increases. And I think that that has settled down now. And part of that is because the marketplace has righted the ship with charging the premium that they've recognized is more of a stable way to stabilize their book and all of the risks putting better controls in place to prevent these hacks from the beginning.

Jeffrey Ziplow:

Got it.

Amy Reese:

So I'm seeing more like a 25% increase in premium, whereas two years ago it was 200%. So good news there, I think.

Jeffrey Ziplow:

Thank God for that.

Amy Reese:

I'm optimistic.

Jeffrey Ziplow:

We're running out of time and I do want to say thank you to both, David, you and Amy, for your insight, your thoughts and your 2023 cyber predictions. I'll be very interested to come back next year, same time, same place, and see what predictions came true and if there's anything new out there. With that, I would like to turn it over to John Gover just to conclude our session.

John Gover:

Yeah, thanks Jeff, and good morning everybody. My name is John Gover and I help lead Cross's independent school practice throughout the Greater Northeast Dane based right here in Connecticut. On behalf of everyone on the call today, we really want to thank all of you for carving out some time on a busy Tuesday morning right before the holidays. First and foremost, we'd like to continue to do these throughout 2023. And so if anyone has any feedback or additional comments, please let us know. So the reality is cyber hygiene is a team sport and it takes a coordinated effort of internal and external resources as well as a properly designed insurance program to protect the institution. If anyone on this call can be a resource or even a sounding board on how you may view this risk, please don't hesitate to reach out to any of us. Lastly, have a wonderful holiday season and an even better 2023. Thank you all for joining.

Jeffrey Ziplow:

Thank you all.

presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgement. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor.