Cyber Threats to Your Practice Webinar

Mike Whitmer:

Good afternoon, and thank you for joining us. My name is Mike Whitmer with NCMIC, and I'm going to be moderating today's discussion. Our topic today is about cybersecurity risk in your practice. This is an important topic because cyber crime is a bigger issue than ever. We hear about it in the news daily and live with the risks. But how can you protect your practice? And is a healthcare practice really a target for cyber criminals?

Mike Whitmer:

To help us dive into this topic, we have Liam Degnan with us. Liam is Director of Strategic Initiatives with Compliancy Group. Liam has a long history in risk management that provides him with a unique understanding into the world of HIPAA compliance. For the last three years, he has advised healthcare decision makers, small practices, and other healthcare vendors, helping to solve and simplify their compliance needs with Compliancy Group. A big part of HIPAA compliance as cyber security, and Liam is an expert. So he's here to help us understand what can be done to protect you and your practice. Liam, thank you so much for joining us.

Liam Degnan:

Hey, it's my pleasure. No, thank you for having me. Happy to be here.

Mike Whitmer:

Good to have you. I really appreciate it. So let's go ahead and dive in. We do hear a lot about cybersecurity. And as I mentioned earlier, it's in the news all the time, hackers, malware, ransomware, lots of scary stuff, especially for people that are not experts in the tech world. Let's start with a very basic level of understanding. What is cybersecurity, and what are the risks to a healthcare practice?

Liam Degnan:

The actual question of what is cybersecurity, it tends to be just a lot more simpler than most people think, because all that means is computer security, whether that's your computers, your devices over the internet, whatever it is. It is security as it relates to your electronic devices, you could say, especially ones that access the internet. In terms of, you could say, the most common risks, especially for a small practice, I'll say the general risks themselves as far as, let's say, bad things that happen, you have, of course, phishing scams and ransomware, which is actually really big, especially among small practices. Roughly 31% of ransomware attacks are actually perpetrated against a small healthcare practice, about 31%. That statistic is only because the information that a small practice has about their patients, especially if they're billing insurance, is extremely valuable information. One single healthcare record can be sold on the black market for anywhere between five and 10 times more than a debit or credit card number because it could be used for identity theft, for blackmail, for lots of other things depending on the nature of the cyber crime.

Liam Degnan:

And so, healthcare practices become a target because they tend to have a lot of valuable information about the patients that they're seeing. But they are vulnerable because they're a small business. Let's say, in terms of the overall scope of things, generally, the biggest risk that a practice faces is human error. It's very rare that you see somebody gets purely straight-up hacked. It's most of the time they get a link in their email that somebody clicks on without thinking about it because it was a deceptive tactic by a hacker that then enabled them to have access to their network. And so, that-

Mike Whitmer:

You know-

Liam Degnan:

Yeah-

Mike Whitmer:

Go ahead. Sorry, go ahead.

Liam Degnan:

I was just saying that tends to be what we see as the greatest risk that small practices face right now.

Mike Whitmer:

To me, it's counterintuitive because small businesses, small practices, I would think that cyber criminals would have bigger fish to fry, that they would be wanting to go after the really big companies that have lots of information and lots and lots of money, that that's where they would focus their attention. But I understand that that's not the case, that small businesses are very much a target.

Liam Degnan:

It's mostly because small business is just an easier target.

Mike Whitmer:

I see.

Liam Degnan:

If you think about it, if I'm trying to pull off a bank robbery, Chase Bank might not be my best bet unless I am an extremely sophisticated, knowledgeable, you could call, a criminal within that arena. But the local small branch, mom-and-pop shop that is up the road from me is a much easier target because it's a lot more likely that they will be less secure than the big corporation would pay. And so, it makes them more vulnerable.

Mike Whitmer:

Sure. I would guess that mom-and-pop shop, for lack of a better term, small business, small healthcare practice may not have the protocols in place to protect, the training, the processes, the security behind the scenes, that sort of thing. I would imagine that the small businesses may not have as much of that in place and that makes them low hanging fruit.

Liam Degnan:

Yeah, and it's also they either... It's not even, let's say, negligence, usually. It's just that if you're the owner of a practice, that's not your area of expertise, right?

Mike Whitmer:

Right.

Liam Degnan:

And you may not have the resources to hire somebody or to outsource or to have everything mapped out. And so, to us, especially for small practices, there's some really simple things that you could be leveraging just to reduce your own levels of risk and [inaudible 00:06:11].

Mike Whitmer:

Before we get into those, first of all, let's start with what scams are out there. You mentioned earlier phishing. That's one. Could you go through some of these and explain what they are?

Liam Degnan:

Yeah. I'll start with maybe giving a more in-depth explanation of a phishing scam, because a phishing scam is really what tends to be the outlet for all of the other types of scams that are out there. So phishing is what leads to malware, ransomware, viruses, because it's the easiest and the simplest way for somebody to get access to your network. And so, basically, if I'm a cyber predator, the way that I'm pulling off a phishing scam is I create a fake email. It could be CEO at the company that you're working at, or it could be owner at the name of your practice.com, something like that. I send an email out to all of your employees, so everybody in your staff, I send them all an email pretending to be, let's say, you as the owner of the practice. In that email I say, "Hey, so-and-so, if you could click this link, we'd like to purchase gift cards for the team as part of Christmas bonus, and you could use the practice credit card to do that." You click on that link, you start plugging in your information. Right after you click on that link, maybe without even realizing it or granting access to your system, by that predator to then come in and either infect it with malware or virus, whatever it is. What's most common is something called ransomware.

Mike Whitmer:

Talk to me about that, because I hear about this on the news all the time, and it's scary.

Liam Degnan:

Ransomware, most recently there was I think with the Pipeline issue, which was a ransomware attack. And so, you'll hear about it with a lot of the big corporations. Usually ransomware is a very small business type of thing. It's mostly small businesses that are hit with ransomware attacks, again, because they tend to be the easier targets. What happens when you get a ransomware attack, let's say that you click on that link and you weren't supposed to and somebody grants access to your system, what happens is they will actually encrypt all of the data on your network, and in order for you to get access to it again, you have to pay that cyber predator X amount of dollars to get access to it. A lot of the time, the cyber predators won't even make it be for that much money. We're not talking about millions of dollars here. I think that the average ransomware attack, it ranges, actually could be as little as $1,000, could be as much as 50 grand, but somewhere in that range, especially amongst small businesses.

Liam Degnan:

And so, what happens is a lot of people will pay the ransom. So let's say it's $3,000, you pay the $3,000 so you can get access to your system. The majority of the time, you never get access back to the system. The predator just runs away with your money and then you need to report it to the FBI or whatever in order to figure out what happened. Even, let's say, among ransomware attacks, the biggest risk is not even that you have to pay the ransom and that you lose that money, the biggest risk is actually the downtime. So your entire database, all of your patients, their names, their emails, their records, their insurance information, all of these things that you've built up on throughout your years being in practice is now gone. You can't get access to it anymore. The downtime that that causes is more expensive to a small practice than absolutely anything else, because it could take a month for them to be able to get the business back off the ground and they don't have any way of then reaching out to their existing patient base to notify them of what happened, because everything was encrypted. And so, ransomware could be really, really messy. It's the biggest one that, let's say, among small practices, the biggest way that you can be compromised.

Mike Whitmer:

Okay. Talk to me a little bit about another term that I've heard quite a bit about is malware, because that's something else that they can get into your system through a phishing scam, something like that. Once you click on that link in that bad email and then malware, what does that do?

Liam Degnan:

Yeah, well, ransomware is a form of malware.

Mike Whitmer:

Oh, okay.

Liam Degnan:

So all that ransomware is malware where your data gets encrypted and you have to pay somebody in order to get access to it again. Malware and different types of viruses tends to be more malicious but less smart because you might get a malware attack and it affects your system and it makes your life a headache for a while as you're trying to figure out how to get rid of it, but there's not somebody on the other end of it saying, "You need to pay me to be able to do this." It's somebody causing trouble on the internet, creating problems and all sorts of other things. Malware and viruses actually tend to be a little bit of a simpler fix compared to something like ransomware.

Mike Whitmer:

All right. There's a lot of risk out there. There's a lot of bad operators that are trying to break into healthcare practices through cyber attacks. What can doctors do to prevent a cyber attack or a scam from impacting their practice?

Liam Degnan:

There's a couple of different layers to the question, so I'll start with, let's say, the actual technology that you have in and of itself, some best practices that you could utilize, because in general, it always helps to have even the most basic of antivirus and anti-malware software installed on your systems. It's not expensive at all. And so, having it there gives you a layer of protection just to make sure that you're avoiding those types of issues.

Liam Degnan:

Now, the second thing is actually a backup, and having a really good backup for your practice is probably the number one way that you could protect yourself from a ransomware attack in terms of being able to recover if it happens. Let's say, if you have a good backup, either in the cloud or stored locally, you should have maybe two or three different copies of your information through different sources, through your EHR, things like that. Even if, let's say, a ransomware attack happens and you lose all that information, you'll be able to restore everything from your backup. That is one of the best things that every practice can implement, is a good solid backup mechanism that they've tested so that they know they can recover their data if something happens.

Liam Degnan:

Now, the other layer to it is prevention. That's more like, if something happens, you should have antivirus, anti-malware, you should have a backup that way you can recover if, let's say, the worst thing occurs. In terms of prevention, the best thing that you could do is actually train your staff. Even a basic cybersecurity training that you have all of your employees go through, that you go through yourself is, believe it or not, an unbelievably effective way of mitigating your risk from a ransomware attack. Statistically speaking, 96% of all companies that were victimized in ransomware attack had antivirus and anti-malware software installed, roughly

96% of them, because most computers already have it. Only 14% of them had actually done cybersecurity training.

Mike Whitmer:

I see.

Liam Degnan:

So it is a really significant reduction in your risk because if you can make sure that your staff is knowledgeable, even if it's as simple as training your staff on how to recognize a phishing scam, having them go through a training, testing it, there's a lot of companies that do that, it can be a great way of ensuring that it never even happens in the first place. And then worst-case scenario, you have that backup in place.

Mike Whitmer:

I know that here at NCMIC, every once in a while, we will get an email that looks bad and they're being sent out by our IT team to test us. It is disappointing because I will admit, I've been caught. I've clicked through on one or more of those. And then it pops up a message, "This was a test you failed." But it is effective, and that really does get me and others here at NCMIC really thinking about these emails that are coming in so that we think twice about clicking on them. I think I'm getting better.

Liam Degnan:

That's good. And it's not expensive to implement. The basic training and the phishing testing, there's a lot of source resources out there that can do that pretty affordably. So it's not a bad idea.

Mike Whitmer:

I think that a lot of our listeners out there are just like me in that I just use my computer. I don't know what's going on behind the scenes to make that work. So if there is a breach, if my system's been compromised whether that's... Ransomware I understand is probably pretty obvious that you have a problem. But other types of malware and viruses, that sort of thing, what are the signs that my system has been infiltrated?

Liam Degnan:

In general, just a good rule of thumb is you want to be looking out for anything that just seems weird, is the easiest way to put it. If you go to log in to one of your systems and you notice that your password has changed, you don't remember changing your password, if you start getting tons of popups showing up on your computer, if you're using your computer and it feels dramatically slower than it used to and there's no definitive cause of why it's being so slow, usually that's an indicator that there's something that's happened. You could take one or more of those signals or multiple slope performance, lots of popups, a random password change that

you don't remember making, and if you see that that's happened, those are usually some good indicators, let's say, that there's an issue.

Mike Whitmer:

Yep. So if it doesn't feel right, there's probably an issue, right?

Liam Degnan:

Yeah, absolutely.

Mike Whitmer:

Or quite possibly, yeah.

Liam Degnan:

Yeah, quite possibly.

Mike Whitmer:

Now I've noticed my system isn't acting right and I suspect that I have a problem, what do I do? What steps should I take when I notice that something unusual is happening?

Liam Degnan:

There's a couple of things. I'll keep this as simple as possible. Most computers, if you are even sitting down at your laptop right now listening to this webinar, most computers have some sort of antivirus anti-malware software running on them in the background. A lot of times you get a ton of little reminders about that because it'll come with something free, and they'll be harassing you, kind of, to upgrade to a better version of it. Sure, why not, right? And so, most people have that level of familiarity, but if you notice that things like that are happening, you're getting tons of popups, your computer's slow, you're noticing strange things going on with your different systems, more than likely that means that the malware has already surpassed the existing protection that you have in place.

Liam Degnan:

So there's two pretty simple steps that you could take. First is, go online and install a new antivirus, anti-malware product onto your computer. There's tons of them out there, a lot of them are even free, but you might want to go with a paid one if you think that there's something going on. They're not expensive. Once you install that antivirus and anti-malware software, shut your Wi-Fi off. So either locally disconnect your computer from the internet and shut your Wi-Fi off there, or unplug your router. Because what happens is, if your computer has, let's say, even ransomware, if there's a virus, if there's malware and it's starting to infect the system, if there is somebody on the other end of that, what commonly happens is they will be installing software on your computer that allows them to control it remotely, which is where a lot of the issues, a lot of the pop-ups start coming, is they've already installed things on your computer via the internet. Shutting your Wi-Fi off prevents anything like that from continuing

to happen. And now that you have that new antivirus, anti-malware software program installed, run it while your computer is disconnected from the internet, see what it identifies. And then once that new program has run, it should allow you to clear it out of your system as far as any potential viruses or malware that might be there.

Mike Whitmer:

So, if I am a doc and maybe I got a weird password changed that I don't recognize, one of those red flags that you just told us about, let's not overestimate my technical abilities-

Liam Degnan:

Sure.

Mike Whitmer:

... are there any resources out there that could help me with this? Do I need to take this to the Geek Squad? If I'm not comfortable with troubleshooting this and working through this, what are some types of resources that are out there that could help?

Liam Degnan:

If you don't feel comfortable or you feel like there could be a potential risk, it's always good to reach out to an expert. A lot of times, even if you just do a little Google search on local IT companies near you, IT companies especially, very common for them to have experience working with healthcare practices. So especially within the IT space, calling an IT company or another name that's very common is a managed service provider, like an MSP or an IT provider, call them, let them know what's going on, and a lot of them will be able to give you, let's say, good input and advice and help you install some of the systems that you need in place to be able to make sure that your system is protected.

Mike Whitmer:

Yeah, okay. I know that a lot of our doctors, our listeners have agreements in place with vendors to perform certain functions in their practice. I'm not talking about those IT resources that can help in a situation like this, I'm talking about just the everyday vendors that people have working with their practice to perform certain functions for their practice, and some of them have access to systems and to patient information, what obligations do vendors have to keep our systems safe?

Liam Degnan:

This is one area where there is a little bit of overlap between, let's say, cybersecurity best practices and the HIPAA rules. There's something called the Omnibus Rule under HIPAA, which is a requirement that if you are working with a vendor that has access to your patient's information, any of your systems, they're considered under the law to be what's called a business associate, and you are expected to actually get them to make sure that they

themselves are able to protect that information and to have a business associate agreement in place with them.

Liam Degnan:

The overwhelming majority of the vendors that you'll be using, like your practice management software, your EHR, even your email, if you're using Gmail, things like that, Outlook, whatever it is, a lot of those companies will automatically sign a business associate agreement with you as part of your onboarding process. And if you have a vendor that is signing a business associate agreement and you have that on file, that's a good indicator that they know what they're doing, let's say, from a privacy and from a security perspective. And so, a good double check, let's say, in your vendors is to make sure that you have those business associated agreements on file with each of those vendors you might be using. That's a big part of the HIPAA rules, and it was a big driver actually for a lot of the government enforcement efforts as far as HIPAA is concerned.

Mike Whitmer:

You have mentioned HIPAA, and Compliancy Group, I know, does a lot with HIPAA compliance. It seems like cybersecurity and HIPAA are really intertwined, that there's a lot of overlap there. So talk to us a little bit about HIPAA's role in cybersecurity, if there is one.

Liam Degnan:

Yeah, so HIPAA is an interesting. Sometimes especially for a small practice, it could be difficult to figure out the ways that the law applies to them because the HIPAA rules themselves are written in a way that's almost intentionally vague because of how broad they are. So, the regs themselves apply to the large hospital groups, the insurance companies, along with what might be a small private practice. What the HIPAA rules require, which is again, really just another best practice from a cybersecurity perspective, is an annual risk assessment. As part of the HIPAA rules, already within your practice, you should be doing some type of an annual assessment on your practice where you review your existing policies, procedures, and training with your staff. If there's no cybersecurity components in there, you might want to add that. That would be something that you identify in that assessment, where you're looking at your IT systems to make sure that everything's encrypted, that it's backed up, that you have those established processes in place.

Liam Degnan:

What HIPAA requires is really just that you do that assessment, that you figure out where your potential gaps are, and that you then make a good faith effort to address those gaps. The majority of what the law requires is more administrative in nature. It's things that you should be doing with your staff, making sure that they're reviewing your policies, making sure that they're receiving trainings. There's the BAAs with outside vendors. The majority of the breaches in the United States, period, about 86% of them are human error related. Because even if it's a ransomware attack, somebody has to click on that link to give them access to your system.

Liam Degnan:

And so, a lot of the HIPAA rules are devoted to more administrative processes that you can implement to make sure that you're doing a checkup once per year and then that you're implementing the necessary measures just to protect yourself and your patient's data. And so-

Mike Whitmer:

Sure.

Liam Degnan:

If you've never done it, a great place to begin is actually conducting that assessment for HIPAA to figure out which you might be missing and then going from there.

Mike Whitmer:

Yeah, good takeaways. What I've heard today as far as takeaways, training is key, training staff, backup is key. Make sure that you are backing up regularly, doing it right so that if something does happen to your system, you can restore that and minimize that downtime. So really good impacts. We talked a little bit earlier about if a cyber crime is perpetrated on a practice, one of the big impacts could be downtime. I would imagine that there are other significant impacts impacting everything from patient care to legal issues. Any of those that you can mention as far as the impact and why we want to prevent this?

Liam Degnan:

There's a lot of layers to it, because if you have a breach, there's first, let's say, liability. From a liability perspective, most general liability insurance policies actually have exclusions that will specifically exclude coverages applying to cyber-related issues, okay?

Mike Whitmer:

Okay.

Liam Degnan:

So things like that as far as the cyber coverage side of things, if there are liability implications, if a patient is suing you due to their loss of information, they felt like their privacy was compromised, it's always good to have some type of a cyber liability insurance policy in place because that can limit the impact there. The reverse side of that is less from, let's say, the legal liability side and actually more from a government enforcement perspective, because under HIPAA there's the breach notification rule. If you have a breach on an annual basis, you're required to report what might have happened. And if you do that, if the government is usually lenient, right, it's always good to report your breaches, but let's say a breach goes unreported and a patient files a complaint against you to Health and Human Services, the government does have the right to then send you an audit and ask you questions about your compliance and your security programs to make sure that you have all of these things in place.

Liam Degnan:

And so, usually for a small practice, that could be a monetary penalty. A lot of times, it's actually a settlement where the government will be monitoring you for a period of two years and you need to be submitting these quarterly reports to them, which could be a big headache in of itself. So there's liability, then there's just the general headache of dealing, let's say, with government enforcement efforts for things like patient privacy, which is a whole nother level on that front.

Mike Whitmer:

All right. Well, thank you, Liam. That's been really good information just for my purposes, better understanding this issue that we hear so much about. We have had a few questions come in from our listeners, so I want to get to a few of those. First one, "How often do you have to renew associate agreements, those vendor relationships, those agreements?" When we sign on with a vendor, you enact those agreements one and done, or is this something that needs to be renewed periodically?

Liam Degnan:

Yeah, so the nice thing with the business associate agreement is once you sign it with a vendor, you don't ever need to do it again unless the scope of services changes. So if I'm purchasing services from a vendor and I sign a BAA, but then I upgrade to some additional other services that they're providing, there should be a new business associated agreement signed that includes that in the scope of work. And so, that would be the only time that you ever need to renew a BAA. Otherwise, you just have to review them once per year, is what the government asks.

Mike Whitmer:

All right. Another one is questioning about small healthcare practices, why are they a target? Okay, we've got this information, but what are they going to do with that information if they're successful getting in? They're going to get name, address, phone number, insurance id. I'm sure some systems are housing Social Security numbers and payment information. But the question is about why are we such a target and what are they going to do with this information?

Liam Degnan:

Yeah, so I'll say in your case, and I think I'm seeing the question that you're referring to, Mike, and I believe, let's say, if you're not billing insurance, your risk level is significantly lower. Okay.

Mike Whitmer:

Oh, I see.

Liam Degnan:

So if you tell me, "In my practice, I'm private pay. The overwhelming majority of my patients not being billed through insurance," your risk level is going to be significantly less because you are going-

Mike Whitmer:

So-

Liam Degnan:

Yeah.

Mike Whitmer:

When you say your risk level, are you talking risk of getting attacked in the first place or risk of negative impacts if you are because there's not that much information for them to get?

Liam Degnan:

Both. Because technically speaking, even for HIPAA, in order to be a covered entity under HIPAA, you have to be billing insurance. And so, if you're not billing insurance, that already reduces your risk level substantially.

Mike Whitmer:

I see.

Liam Degnan:

And it's also just less information that they'll be getting access to.

Mike Whitmer:

I see.

Liam Degnan:

Now, if you have insurance information, if you have Social Security numbers, if you have all of that information, that becomes very valuable to a cyber predator. The trouble is that sometimes a cyber predator is not going to know whether or not your practice is billing insurance. They're just targeting a thousand practices across the country that they think are easy targets. And so, your risk level is lower, let's say, from a liability perspective, because by nature you have less information about your patients. But if you're billing insurance, your risk level is higher because there's HIPAA implications there, breach notification, and it's a lot more data that that cyber predator would be getting access to.

Mike Whitmer:

I see. Okay. Thank you. One here, "If attacked, what agencies must you report to?"

Liam Degnan:

The Office for Civil Rights is the enforcement body of Health and Human Services. So if you go to hhs.gov, there is actually a section on that website related to breach reporting. It is just like a form that you fill out once per year related to any incidences that you had throughout that year, and that gets actually filed with the OCR. So if you go to hhs.gov, they have a ton of information related to that. It would be ultimately reported to Health and Human Services and the OCR.

Mike Whitmer:

And along those lines, earlier you were talking about a ransomware attack and you ran through a scenario where practice gets hit with a ransomware attack, they pay it, and they still don't get their information, then they go to the FBI. If you have a ransomware attack, what are the first steps? I mean, should you just call the FBI immediately? What do you recommend there for I've got a ransomware on my screen, what do I do?

Liam Degnan:

It's always good to notify the local authorities, so even your local police department, which will usually involve the FBI if it's a ransomware attack. Of course, this depends on the sophistication and the level of the attack. So a lot of the times, if you have a backup, there's two things. If all of your data is encrypted and you have a backup, even if you have a ransomware attack and somebody has encrypted everything in your system, it's not, technically speaking, a breach because the data was encrypted to begin with. So even though they encrypted your system, they can't get access to your patient's information. There are sometimes ways around that, which is why there's lots of different types of encryption methodologies, but as long as you know that that's in place, it's a great way to be. Right?

Mike Whitmer:

Okay.

Liam Degnan:

Now, the other aspect of it is if that does happen and you don't have proof that the data was encrypted, it's very important, big part of the HIPAA rules is documenting those processes, so if you know that everything is encrypted, you should do a risk assessment where you actually then document what's encrypted, what's not, make sure that that's clear on your systems. And then getting the OCR involved, notifying them of the incident as well as the FBI, that's the way to go usually.

Mike Whitmer:

Got it. Okay. Backups, you've talked about that several times today. Question is, "Any concerns about doing cloud backup? Is it okay to do that, or do you recommend external hard drive only?" What do you recommend?

Liam Degnan:

So there's something, and this is, again, considered cybersecurity best practice, there's something called the 3-2-1 rule, meaning you should have three copies of the data, so let's say, what currently lives in your computer, and then two additional copies. The two part is that they should be two different methods that you use. So cloud backup is good, but also actually having it on an external hard drive is not a bad thing. And then the one rule is that one of those copies should be far away from your existing physical location. That way, let's say your practice burns down and you have everything on an external hard drive in the practice location, that backup can't help you, right?

Mike Whitmer:

Right.

Liam Degnan:

So having three copies of your information, let's say your computer, the cloud, and an external hard drive, is the most secure and efficient way to make sure that's all being protected.

Mike Whitmer:

Okay, great. Thank you. Any questions? All right, I think that we're going to go ahead and stop there.

Mike Whitmer:

Liam, thank you so much. This has been really helpful. I've gotten a lot of good information just for my information as a computer user both here at work and at home. This has been really helpful. I really appreciate it. Before we go, I would like to remind our listeners of the resources page on ncmic.com. Today's webinar is going to be posted there as soon as we get that processed and posted, so keep an eye out for that. You can also keep up to date on new resources from NCMIC by following us on Facebook, Twitter, LinkedIn, and Instagram. We're always adding resources to our website, and we typically post those things out on our social media channels to make people aware. So they're out there, we hope you use them. That's it for today. I would like to, once again, thank Liam for joining us today. This has been really helpful in understanding these issues. I'd like to thank all of our attendees. Thank you for listening, appreciate it, and we will see you next time.