Talk to Me About A&E: Episode 5

ALEX RICARDO: Ransomware, I hacked in, I lock up your data and say pay me. And so, for that reason, we're going to likely see any size company, any type of industry be in the crosshairs.

SPEAKER: Welcome to Talk to Me About A&E, a podcast series focused on risk management for architects and engineers. Host, Dan Buelow, Managing Director of Willis A&E will engage experts across the A&E spectrum on topics ranging from contract details to the broadest trends impacting design professionals in North America.

DAN BUELOW: Hello and welcome to Talk to Me About A&E, a Willis A&E podcast series where we focus on a specific risk management topic for architects and engineers. I'm Dan Buelow, Managing Director of Willis A&E.

And our topic today is on cyber liability, and what design firms need to be doing when it comes to managing this evolving risk. My guest today is Alex Ricardo who serves Beazley's cyber and executive risk focus group. Hello, Alex, how are you doing?

ALEX RICARDO: Hey, Dan, great to be here, and thanks for having me.

DAN BUELOW: Absolutely great to have you. Now, Alex has been on one of our Willis A&E on-demand programs which is available as well, which is an hour and a half program. But we wanted to bring him back here for more of a succinct short discussion around this critical topic of cyber liability.

The cyber liability market is by far the hardest market in the property casualty insurance marketplace, and that's going into 2022 here. Meaning, design firms are seeing significant rate increases and even difficulty in securing the coverage they need, and in some cases to meet their contractual requirements.

Our Willis Towers Watson cyber team puts out a quarterly market report. And the last report that came out stated that we can expect a continued hardening of the cyber liability marketplace.

And that the average renewal increases are ranging somewhere around the neighborhood of 70 to 200 plus percent, and it's sometimes higher than that, particularly for underpriced programs, and when security controls are lacking for challenged industry classes. And, oh, by the way, guess what, construction in A&E are considered challenged industry. Meaning, they are seeing a lot of claims coming out of this sector.

So, what is driving this and what can design firms do to mitigate their cyber liability risk? This is a very important question and fortunately, we have Alex here today to help us answer this question. So, let me tell you a little bit about Alex.

So, Alex Ricardo is based in New York City and provide support and guidance to Beazley's insured base from both a breach preparedness and breach response perspective. Alex has over 20 years background of service to Fortune 500 corporations and government agencies, addressing information leakage prevention, data e-discovery, messaging encryption, internal threat management.

And Alex is a Certified Information Privacy Professionals, CIPP, for the US, which is a credential issued by the International Association of Privacy Professionals, IAPP. This credential demonstrates Alex's breadth of knowledge on privacy principles, general privacy law and information security, best practices throughout the United States and the world.

Prior to joining Beazley, Alex worked with Kroll Inc, a leading global security and risk management company where he was their privacy subject matter expert and zone leader for the data breach service group. And so, we're lucky to have Alex.

And one of the things that with these programs, I think it's important for any leader of a design firm to be listening to this and getting this type of information. But you also definitely need to plug-in your IT folks and anybody that consults on your behalf in this area because it is certainly highly specialized.

So, Alex, let's start off here with this question here. The cyber marketplace is very young, right? In fact, it was only a few plus years ago when A&E firms started even purchasing a standalone cyber liability policy.

And in fact, many question a design firm cyber liability exposure the target breach in 2013 was the big event that captured a lot of attention after hackers stole over 40 million credit cards, and we saw $18 million of a settlement. But most design professional firms really don't have much of any of that exposure.

But things have changed dramatically in the last year or two, and we are now in what we could be described as a hacking era. And what are some of the ways cyber liability and risk has evolved over the years, Alex, and why has ransomware become an emerging risk in the last several years?

ALEX RICARDO: Great question, Dan. So cyber risk has evolved so many ways over the last couple of decades. The whole concept of cyber risk, in general, probably began with the dawn of the internet, back in the mid-90s.

So back then, the big concerns that most cyber underwriters were concerned around were primarily things like viruses, denial of service attacks. This is back in the days of when eBay, and Amazon, and other e-tailers started to come to fruition.

And then everyone got nervous with Y2K, and that term became the buzz term for a few years. And we all survived it, we got past it. And then a nuisance factor emerged called spam. And then we had to deal with various technologies that help prevent spam. Then 2003 came around, and that's when the first privacy notification law came on the books.

California introduced SB 1386, and that was the real beginning, if you will, of what I would call the modern cyber risk that we see today with hacks. Hacks take on a variety of flavors; data breaches just happen to be one of them. But everything from ransomware, crypto jacking, other types of hacking perils can occur.

And that's been the big concern with cyber underwriters lately is how the compounded risk of multiple perils on one single hacking event is what's keeping them up at night. And so, ransomware is the current flavor, that's the flavor of the day right now, and it has been for several years. And so, with that, that is where we're seeing the primary emerging risk occurring is with ransomware.

It is an efficient way for hackers to make money, which is why that has been the pain point, if you will, for the last several years. Data breaches, if you can envision, we would have to hack in, look for private or sensitive data, exfiltrate it, and then go to a dark web, for example, and find a buyer.

That's a lot of hoops for the attacker to go through in order to get money in their pockets. Ransomware, I hacked in, I lock up your data and say pay me. And so, for that reason, we're going to likely see any size company any type of industry be in the crosshairs.

DAN BUELOW: And that's really kind of why we're seeing this resetting, if you will, of the insurance marketplace. It really, when they were establishing pricing and trying to figure out how best to underwrite this risk, a lot of this ransomware exposure really wasn't contemplated, I think, is what we're kind of seeing here.

So, when you see about 70% or 100% or 200% rate increases, because some of the premiums that we were seeing were very low. I mean, you could see 10,000, 7,000, 10,000 15,000-dollar premiums pretty sizable accounts, if you will, from an A&E sector. It doesn't seem like it takes much to have a claim that's going to move the needle on the loss ratio on something like that.

ALEX RICARDO: As we always say, cyber risk is still an ever-evolving risk. It is a moving target every day, in fact. We could be having this podcast six months from now, and we could have a whole different discussion around the risk landscape. But the primary driver probably for the last couple of years, again, is this concept of compounded risk.

And unfortunately, what the underwriters have started to see is how that single hacking event can cause the attackers or the actors to start looking at "Well, if I'm already in here, let me do

ransomware." "Hey, while I'm doing ransomware, nothing says I can't go look for data and steal it and have a data breach."

"Hey, while I'm at it, I can also do crypto jacking and use this company's CPU power to go mine for cryptocurrency" and the list goes on, the possibilities are endless in that capacity. So that is what's been sort of surfacing in the last couple of years. And with that, it's going to cause an involvement of how the cyber underwriters underwrite the risk these days.

DAN BUELOW: And again, Willis A&E, we strongly recommend a standalone cyber policy. But as we'll get into this, that really is your second line of defense, your first are these robust IT practices, and we'll get into that and talk about that.

But you need to keep in mind that these cyber liability policies will be covering your first- and third-party exposures. And arguably, a design firm could count on having some third-party coverage for cyber-related incidents, but that's not-- again, as we get into this where we're seeing these claims coming in, we're seeing these as first party, and you don't have any coverage anywhere else for first party.

And what we're also seeing is some of these carriers starting to say "Well, we don't want to have these third-party exposures." And so, you're going to start seeing some exclusions and certainly some limited reduction of limits, specific to that. So, Alex, let's drill down a little more on this ransomware. How do these hackers commit ransomware?

ALEX RICARDO: Great question, I get asked this quite often. People are fascinated in ways of trying to just understand and get in the mindset or look through the lens of these attackers. It is a complex process.

One of the tools or frameworks we often easily use to describe these attack approaches is what's often referred to as the Cyber Kill Chain. It is just a framework that was devised, oh, my goodness, about a decade ago by Lockheed Martin Corporation.

And what we've done is we use that framework to describe, if you will, what ransomware attackers will go through in order to commit their exploit. They all begin with the initial compromise. So, they essentially have to find a means to get within that network of the company they're targeting.

That can happen in a variety of ways. The most common way is the means of attacking inward. Meaning, going through something like social engineering, spear phishing, causing somebody to click on something, like within an email and an attachment or a link, or a document, and that will allow the attacker to successfully make their compromise.

Sometimes, it can be the other direction where the attacker is going to lure an individual to come to them. The most common one we see, forgive me for bringing it up as an example, will be like a pornographic website.

Having somebody click on a link, click on an image that they're not supposed to. And by doing so, it allows the compromise to occur. We've even seen the most outlandish examples where a set of keys on a keychain are left in a parking lot with a USB drive.

And somebody picks them up and then their good intentions, they want to plug-in, the drive to find the owners of the keys to return the keys. And lo and behold, that was a big mistake, they just injected malware on their computer. All these different examples are ways that compromise can occur.

Once that compromise occurs, then we must establish the communication link, as we would say, or the see-to link is the more technical term, that allows for the outside attacker to communicate into the company now, and now they can do all of their exploits remotely, which clearly is what these attackers want to do.

What they're going to do once they have that communication link established is essentially laterally move through the network. This is their opportunity to explore as many different segments, different parts of the network that they've just targeted.

And the more segments, the more areas of the network they get into, the more leverage ability they have to demand a higher ransom. So, their goal is to really laterally move through as much of the network as they can, and they're doing this all stealthily, they're doing this under the radar, if you will.

All while they're doing this, they're trying to avoid being detected. And now, this is the tightrope walk that every attacker goes through. In their mind they're saying, "Well, I really want to spend another hour, another day exploring this network, because more systems I can get into, the more I can demand a ransom."

But that means, every hour, every day that passes, they risk getting detected and getting locked out. So, they're always weighing it like a tightrope walk to say, "OK, if I satisfied my appetite, if I connected to enough systems."

At some point, every attacker says, "Yeah, I don't want to risk getting detected anymore, I'm ready to run ransomware." And that's when they hit the proverbial red button, encrypt as many systems they've compromised, put on a nice blue screen, and advise the company, "Hey, I have locked up your stuff, you've got to pay me in Bitcoin."

So that sort of describes what these attackers go through, and it is a lot of effort. So, by the time they hit that point of "Hey, you got the ransom demand on the screen," a lot has already happened behind the scenes.

DAN BUELOW: And this is really big business now, isn't it? I mean, it's very sophisticated where these folks are not just these random kids in their basement now, it sounds like you've got like actual businesses running and thriving doing this.

ALEX RICARDO: Yeah, we do. I always jokingly say that years ago, if you wanted to wrangle up all of the hackers, you probably can go to the next Star Trek convention, and you'll probably get them all, you can't do that anymore. These are no doubt, organized crime units, very sophisticated, heavily funded.

If we all got on a plane and went out to Eastern Europe, or Russia, or the Ukraine, or Southeast Asia where predominant number of these crime rings exist, they're all sitting in office towers, probably much like you and I do, sitting at cubicles. They probably get benefits; they get a payroll check and vacation time and everything else that we get.

And they're obviously sitting in jurisdictions where those governments turn a blind's eye, no doubt. So unfortunately, this is a very sophisticated crime business these days. This is definitely not that lone teenager in mom's basement at 3:00 in the morning.

DAN BUELOW: And these days also, the underwriters will often run these vulnerability scans for their insureds, I believe, and requiring perhaps some remediation of some weaknesses. It's fair to say that these hackers are probably running these same scans to help select their next victims, I'm assuming.

ALEX RICARDO: Yeah, Dan, no, you're spot on. Essentially, with a lot, and obviously, I'll speak generally for the cyber carrier industry, but specifically even at Beazley.

There are cyber carriers now that are taking that proactive approach as part of their underwriting process to look at being able to do some kind of scanning or assessment, if you will, of either prospective insureds or even bound insureds.

Now, the one thing I can say very clearly, all these kinds of scans are what are often referred to as external facing scans. So, in other words, there is no penetration or invasion into a company's network, at least from Beazley's, and that's where we draw the line. So, it's anything that can be seen from the public domain, from the public side.

But that also means, and very much to your point, that's the same kind of scanning these attackers can do looking for vulnerabilities, looking for ways to get in from a vulnerable configuration perhaps that an organization may have put into place. So, whatever we would scan for, it's the same means of scanning that can be done by an attacker.

And so that demonstrates, again, if the cyber carriers can find these low hanging fruits of vulnerabilities, so can the attackers. And if we can just help any insured identify some of those low hanging fruit pieces and hopefully prevent an attacker from finding it, we're at least believing we're doing a service to those insureds.

DAN BUELOW: Absolutely. When it comes to ransoms, isn't it illegal to pay a ransom?

ALEX RICARDO: Yeah, no, good question Dan. So as at the time of the recording of this podcast, there is no federal legislation or laws that prohibit the payment of it with the only exception again being the OFAC sanctioned entities.

It really does come down to being a corporate personal decision or a personal corporate decision. Many companies will weigh that in and out but from a legal standpoint, at least from the US, it's just the OFAC sanctioned entities we need to be concerned about.

DAN BUELOW: We also get this question a lot, is this extortion payment insurable?

ALEX RICARDO: We get asked that quite a bit as well. So yeah, extortion coverage does appear in many cyber policies. Again, it's going to be carrier to carrier, but it is insurable again except where it's not permitted by law. And so, again, once from the US side, it really becomes like the OFAC sanctioned entities.

It is quite rare US entities succumb to ransomware from an OFAC sanctioned entity that does not happen often, thankfully. That's mostly because the entities themselves are aware they're on the sanction list. And so, they're going to target their energies and efforts to companies that are non-US based, where other countries may not have a sanction list for them.

But at times, as I often say, these attackers are not the sharpest knives in the drawer, you may once in a while have an OFAC sanctioned entity, go after a US company, they're unaware of it.

They come to learn the hard way, they've done all these energies and efforts to compromise this company, and then they come to learn they've reached a US entity and now they're not going to get paid. So, it can happen, but it is rare.

DAN BUELOW: And given the fact that these hackers are in your system snooping around, there's a very good chance that they probably have a copy of your insurance policy or standalone cyber liability policy. Where do you safeguard, they keep it under your mattress, or what do you suggest on that?

ALEX RICARDO: It's also a good question. And cyber underwriters have started to notice this over the last couple of years by way of the forensics investigations of active incidents that we've been dealing with over the years. The evidence shows that these attackers are going around, snooping, and sleuthing through the network, looking for evidence of cyber coverage.

And they're doing it because that becomes their floor. They come looking for these limits within the policy to say, "Hey, I don't want to leave money on the table. I want to know what is the minimum I can ask for knowing they got deep pockets to have these paid off."

So, I often tell insureds, although most carriers don't go to the level of like, what some carriers do for K&R coverage, which is you're actually under provisions to not disclose, you have the K&R coverage or confirm you have the coverage.

Cyber carriers, I believe, have not gone to that level, but I often advise clients to go to that level. Even if it's not required in the policy, just do your best to not confirm the coverage as much as you can. We do recognize some entities have to like publicly traded entities under SEC guidance and disclosure.

But if you can keep quiet about the amount of coverage you have, not have it be easily identifiable on your network, that can help offset the advantage, if you will, to these attackers if they were to come across and stumble across the fact that you have the coverage. So, safeguarded as much as you can from the network as possible.

DAN BUELOW: And then these folks like getting paid in Bitcoin, should a company get a Bitcoin wallet for that rainy day?

ALEX RICARDO: So, Bitcoin is the cryptocurrency of choice. Every once in a while, we'll hear about a different cryptocurrency being demanded. But Bitcoin is the go-to currency, if you will. I actually do advise clients not to get a Bitcoin wallet. The primary reason is these Bitcoin wallets, these accounts, they're not so-called FDIC insured.

There is no regulated industry to them, there's no regulatory standard, there's no insurance for these accounts. So, they get hacked into in their own right. So, having the Bitcoin siphoned out before that rainy day occurs is not a good thing, because you're losing out on those funds. So that, to me, is the primary reason why I wouldn't be looking to establishing your own Bitcoin reserve.

The other reason is because there are providers out there that at the time of need, if you had the unfortunate situation where you had to make an extortion payment, there are firms out there that do the payment and facilitate the payment on your behalf. So therefore, they absorb the risk of their own Bitcoin reserve being stolen rather than your organization.

So, for those reasons, we advise clients don't create a Bitcoin wallet, don't get Bitcoin reserve. If you had the need to make a payment, at least from Beazley's. And we would have a payment facilitator and ransom negotiator that help the company through that process.

DAN BUELOW: That's important. And I think as you've noted here, these policies are not all the same, so you've got to know you have for coverage. And. It's changing a lot and the market is definitely continues to change here.

And one of the changes that we've seen this year was the requirement by most carriers now that certain controls are in place before even offering a quote, even a renewal quote. Talk to me about these controls, and what protective measures Beazley is requiring that firms have in place.

ALEX RICARDO: As I mentioned in the beginning of the podcast, the evolvement of this risk, especially in the last couple of years, has really shed light around compounded risk. And the concept of compounded risk is just magnified by certain series of controls that might be lacking at some companies.

And so, what cyber underwriters have started to identify is that there are certain controls that are quite frankly paramount, they're almost essential these days to help avoid a lot of this kind of risk from occurring. So, things like the one that you may hear quite a bit is like multifactor authentication.

And for any of the listeners not familiar with MFA, as we often call it, it's the concept of having a second password to get into a system. So, the first password is one that you may have memorized, but the second password is one that might be a six-digit number that is texted to you after you attempt to log in, for example.

And many of us may have experienced that with maybe our online banking, that second password or second factor, as we say, is the means of helping assure that a system does not get compromised by an attacker.

Because the attacker might steal your password that you memorized, but unless they also stole your physical phone where you're about to get that six-digit pin, for example, it's pretty highly unlikely, they're going to be able to compromise that system.

So, the concept of multifactor authentication has really become quite important from an underwriting standpoint. And so that's just one example of a series of other types of technical controls or security measures that underwriters are going to start looking for and finding to be of importance as part of their underwriting process.

And so yes, in these last year or two, we've started to see where the underwriters have become, quite frankly, a little more scrutinizing in terms of these controls because they recognize the importance of these controls in this era of compounded risk.

DAN BUELOW: Great points. And what's happening here is we're seeing it evolving of the standard of care in order to manage this risk. In design firms, we've had a lot of different claims that would be in that cyber related area. And one we just had recently; I would maybe describe it under this social engineering. I'd like to get your take on this, but what we had was an architect approved a payment application.

And this payment application was identical to the last payment application and that the owner wanted to have the architect sign off the contract or completed this work. The difference was is that where the money was being transferred off at the end of the day went to some offshore account into somebody else's hands.

And you have a very disgruntled owner that arguably made their own share of mistakes, but it's certainly puts the design professional in a precarious position with their client, and also raises the question of the standard of care. Should there be different ways of confirming that this is a valid account? Or this is where the money should go, and so forth, it's a big problem.

ALEX RICARDO: Yeah, I completely agree Dan. One of the things that at least I hear from Beazley's cyber underwriters is having the means of having certain procedures instilled around out-of-band authentication. Some people still go by the old adage "When in doubt, pick up the phone," I'm a firm believer of that.

You get some kind of request, you get something that has been changed in a process by way of email or some communication, electronic communication, and it's different or something has changed in that process. You know what, pick up the phone, verify that, indeed. We've seen a lot of this kind of fraud occur from even like wiring instructions.

So, wire instruction fraud is really escalated as well in the last couple of years. And so, having the ability to instill like an out of band authentication process. You're being asked to wire funds to a new wiring instruction, a new wiring account.

"You know what, let me pick up the phone to a trusted and verified source to confirm if indeed this is a verifiable change, an actual change, or is this a fraudulent change." And so, having those

kinds of simple procedures added can mean a world of difference. So, we definitely are seeing things like that being instilled to help avoid that.

This kind of a transfer, this kind of fraudulent scheme is often what we refer to as a voluntary transfer of funds. Meaning, the company, the victim in this case, voluntarily, in their own right, transfer the funds. Even though the instructions were fraudulent, the transfer is voluntarily done by the company.

Those types of schemes, those kinds of perils often you will see in a cyber policy. The involuntary transfer of funds where the company is not doing it, a hacker got in, and the hacker is executing on the transfer.

Those types of scenarios of perils are usually going to be covered by like a fidelity or crime policy, you generally will not see involuntary transfer of funds coverage within a cyber policy. So, it's just important to know the difference, it's subtle, but yes, you'd be looking to your insurance broker for those subtleties and making sure the right policy is covering the right peril.

DAN BUELOW: Yeah, great points. And it seems that when these ransom attacks occur, it's always at the most inconvenient time. I'll be getting calls on holidays and weekends. They're obviously hoping to catch their victims flat footed, if you will. But firms really need to have some measures in place to be prepared.

We talked about the controls that your underwriters are expecting to have in place to mitigate this. But what are some of the best practices or guidance that you might offer for incidence response to an actual attack?

ALEX RICARDO: Oh, my goodness. I've been in this industry now coming up on 25 years. The largest, most critical, most damaging incidents I've dealt with have always fallen on holidays. It's just the nature of the beast. At the time of our recording of this podcast, we're coming up here on the Christmas holiday period.

Beazley cyber response unit in house, they're all on alert. We just did it for Thanksgiving, we just did it for Labor Day. Every holiday period, it becomes where it's like we're all heightened to expect the unfortunately worst from happening. So that is unfortunately a commonality we've seen for many years now, and it is to the point you outline.

They tend to have less visibility, less vigilance, less monitoring, less resources, monitoring a network, for example, during holiday peak periods. So, the attackers take advantage of that. There are few measures that we often advise clients just to put him in a better position, and a better prepared position for when these kinds of things happen.

So, we're going to do our darndest to help companies avoid having the risk occur, but no company out there can guarantee 100% prevention of these risks. Let's prepare a company for when and if it were to happen. Some of the things I advise clients to do, most fundamental, have a proper incident response plan established.

That is not something that is going to be drafted or created overnight. Companies spend months at times building out and having formulated a response plan. Keep in mind response plans are not just for the IT professionals. Many companies build response plans for the business stakeholders. So, IT professionals maintain their own series of response plans for a series of different types of events.

But the company should have a cyber response plan for the business team. Meaning, the legal folks, the IT folks, the risk management team, you have an HR department that might be involved in some instances with these types of incidents. All of a sudden, you're looking at six to eight stakeholders that go outside of IT.

Well, those are the people that need a plan. They need a game plan to put on the table and say, "OK, what are we about to do and we just had this attack occur?" Those plans having in place have served companies well over the last couple of decades. So, I can't speak, more importantly, about having a proper incident response plan like that in place.

From Beazley's end and I know from all of our peers, all the cyber carriers, they definitely recommend this as well. And just about every top line cyber carrier is going to offer resources around formulating or crafting those plans. And as a company, you want to take advantage of that, definitely have that in place.

The other thing I would recommend is make sure you go through proper tabletop exercises going through the fire drill, test that plan, pull out that plan once or twice a year. Put up a fictitious incident and see how the plan works. Test out the team. Having a prepared team that has gone through regular and routine drills serves far better when the real deal hits.

I have seen it time and time again where a team that has gone through these tabletop exercises, they find themselves in a far better position when the real matter occurs. Also, just as a side note from a regulatory standpoint, if a regulator were to come in to investigate a cyber matter, having demonstrated you go through tabletop exercises and routine drills, put you in a much more favorable light with that regulator.

So again, another reason, in my opinion, another important reason, why you would want to make sure you conduct those exercises. And then test your employees on various things. Many companies these days do what's known as ethical spear phishing exercises.

Essentially, they will send scammed emails to their workforce, and see how many of their employees fall for the scam. And falling for it means it doesn't actually cause harm, but it gives indication that that employee probably clicked on something they shouldn't have and so on. Go through those kinds of triggers.

The more and more you keep your employees on their toes, if you will, the less likely when a scam may get through your IT preventative systems that that employee might be a little more heightened not to click on something they shouldn't have. So again, simple things really can mean a big difference in terms of the preparedness a company has in place, if, in fact, one of these types of risks were to occur.

DAN BUELOW: Very important advice. This last question for you is on what the marketplace is doing, as far as what are companies out there providing. There's so much going on here, the technical challenges in order to obtain this coverage now and to manage it and hopefully keep these costs reasonable. What are carriers in the cyber area these cyber carriers providing in the area of assistance or support?

ALEX RICARDO: What we're starting to see within our industry, at least in the last, I would say a year or two, is we're starting to recognize that, especially for cyber carriers, in this age we're in this evolvement of cyber risk, cyber carriers cannot just provide underwriting and coverage.

They have to go that extra step, they have to go to the level of actually providing risk management services, providing complimentary means to help their clients, their insureds through the process of managing the risk. Again, just three years ago, four years ago, cyber carriers were just purely that.

They were providing cover, they were underwriting, and that was as far as they would typically go. But in this day and age, it really has to be a true partnership. And any cyber carrier that, quite frankly, wants to stay relevant in this climate we're in today, they need to possess that technical competency and truly be a partner with their insured.

They both have a stake in it, quite candidly, they both have a reason to make sure these measures are in place. That just helps that insured be a better risk, which ultimately benefits both the insurer and the insured.

DAN BUELOW: Great advice, great information. And Alex, I want to thank you, this has been very informative. And I really appreciate you sharing these valuable insights with us here today. And I want to recap just a couple of things, I think, is important because as a broker trying to get this information out to our clients.

And to your point, we really got to come together and share information as best we can with the insureds out there. But a few points is that we've been trying to express out over this last year.

And that certain measures and controls must be in place in order to mitigate this risk, and to maintain your cyber liability coverage in the future. That's job one.

And we talked about the MFAs and other controls. Well, we need to be updated on what those controls are, and you should be working with your broker. Well, in advance, these renewals, there's a lot of underwriting scrutiny. Also, things underwriters are swapped, and so what we need to do is get this information to them as soon as possible in order to get a meaningful renewal quote.

And that firms that have cyber related losses are finding renewals very difficult, and the costs are going up extremely high and on a rate basis. Even if it's available, we're seeing a lot of non-renewals. Again, firms need to invest in these controls and have these measures in place in order to reduce the likelihood of such a claim.

And lastly, I would always advise you to check with your broker before accepting any contractual requirements for cyber liability insurance. Limits that are greater than what you currently carry should definitely be confirmed that these limits are available, and commercially viable for you and your firm because we're starting to see more and more contractual requirements.

So, I want to thank again Alex Ricardo from Beazley cyber executive risk focus group. Thanks Alex.

ALEX RICARDO: Thanks, Dan. I really appreciate the invite, great catching up with you.

DAN BUELOW: Great talking to you, Alex. And thank you everyone for joining us for another edition of Talk to Me About A&E, and we'll talk to you soon.

SPEAKER 3: Thank you for joining us for this WTW podcast featuring the latest thinking on the intersection of people, capital, and risk. For more information on Willis A&E and our

educational programs, visit willisae.com. WTW hopes you found the general information provided in this podcast informative and helpful.