Talk to Me About A&E: Episode 11

ALEX RICARDO: People ask me, well, how big should that plan be? As I say, if it's the size of a phone book, it's too big. If it's the size of a leaflet, it's too small. It's got to really have some meat on the bones to be of value to the team. But certainly, you are not looking to create a phone book sized document that clearly no one is going to want to use in the moment of crisis.

[MUSIC PLAYING]

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: Well, hello. And welcome to Talk to Me About A&E. I'm Dan Buelow. And our topic today is on developing a cyber incident response plan. I chair the cyber subcommittee for the National ACEC Risk Management Committee. And I asked a couple of my fellow subcommittee members, Carter Boardman, and Alex Ricardo, to talk to me about why developing an incident response plan is so important for any design professional firm and what goes into these plans. Welcome, Carter and Alex, to Talk to Me About A&E.

CARTER BOARDMAN: Hey, Dan. Thank you.

ALEX RICARDO: Thanks, Dan. Great to be back.

DAN BUELOW: Carter Boardman has over 45 years of contract, subcontract administration experience on a wide range of engineering and construction projects. And Carter presently works for Merrick & Company, a large engineering firm based out of Colorado, as their vice president of contracts and risk management. And Carter is the past president and board of director of the Risk Insurance Management Society-- RIMS-- Rocky Mountain chapter. Welcome, Carter.

CARTER BOARDMAN: Thank you, Dan. Glad to be here.

DAN BUELOW: It's great to have you. In addition to Carter's significant experience as a risk manager for a design firm, Carter has some real-life experience in dealing with a cyber-attack on his firm and in developing an incident response plan for his firm to better prepare for any future attacks or cyber incidents. So, we are very fortunate to have Carter here for this discussion.

And Alex Ricardo serves as Beazley's cyber executive risk focus group with managing business and development initiatives for Beazley's Breach Response program. Alex is based in New York City and provides support and guidance to Beazley insured base from both a breach preparedness and breach response perspective. Alex's background in risk management as well as the software industry and combined with his extensive knowledge of security threats and mitigation best practices assures his clients of a comprehensive problem-solving approach. And we've had Alex on our earlier program on this topic of cyber in which Alex shared his expertise on this evolving risk of cyber liability and specifically ransomware attacks and offered some practical advice on what controls design firms need to have in place to mitigate this risk and qualify for insurance in a hard cyber insurance marketplace.

In this podcast, I wanted to talk about what a firm needs to be prepared for in the event of an actual cyber incident that impacts their business. What exactly will you do when your systems have been compromised, and there is an attack or cyber related incident that jeopardizes your entire business practice? What exactly do you do? And who all in your management team must be prepared for this very event?

It's also worth noting that while it may not be mandated that a design firm have an incident response plan in place, we have seen underwriters in the insurance industry now offer credits for firms that have these plans in place. But regardless, we would recommend having a formal incident response plan in place for any design firm as sound risk management practice. So, Alex, let's start off by giving us maybe an overview on what is an incident response plan. And fundamentally, what are some of the high-level best practices towards crafting such a plan?

ALEX RICARDO: Yeah, Dan. There are different types of response plans. Fundamentally think of it as two different types. One of them, which is the more common one, is the one that's focused mostly for the IT professionals. Those are the kinds of plans that get fairly technical. They're really meant from a containment and remediation standpoint and what IT professionals often have to go through when, let's say, a cyber incident is discovered.

The other plan, which I think, in my humble opinion, is even more important, is the non-IT plan. We often refer to it as the business stakeholder plan. It's essentially the rule book. It's the plan of attack. What does the executive team that is now gathered about a cyber incident, what do they have to go through from a phased approach to managing the incident and then working in concert with the IT professionals through the actual incident itself?

Some best practices that I often share with clients very fundamentally about those kinds of plans, always recognize it's a living and breathing document. You may put one together, invest a lot of time and energy to get one drafted and finalized. But I hate to say it. It's not one and done where it's now a static document that sits on the shelf forever and a day. It is going to be evolved just as cyber risk evolves. So, it is a living and breathing document that will be routinely updated and kept current.

The other thing I recommend is the plan's got to be clear and easy to be used in a moment of crisis. So, keeping it succinct, organized by sections makes it a much more usable document when the incident occurs.

And as I always like to say, people ask me, well, how big should that plan be? As I say, if it's the size of a phone book, it's too big. If it's the size of a leaflet, it's too small. It's got to really have some meat on the bones to be of value to the team. But certainly, are not looking to create a phone book sized document that clearly no one is going to want to use in the moment of crisis. So just keep some of those tips in mind as you're crafting and building that plan.

DAN BUELOW: So, Alex, are there any laws or regulations that mandate having an incident response plan? And how might these impact design firms?

ALEX RICARDO: Yeah, Dan. Obviously, in fair disclosure to your audience, I'm not a lawyer. I'm not an attorney. However, there are certain regulations that will, in fact, mandate having an incident response plan in place.

Not to go into the full extent, but some of those laws that may impact design firms, believe it or not, one of them would be HIPAA. If your client self-ensures their medical benefits for their employees, that actually is characteristic that that data set within HR is viewed as PHI under HIPAA law. So, we do see, in fact, some non-health care entities being HIPAA entities. So, keep that in mind. If that qualifies you, HIPAA does have a mandate in their law to have a written incident response plan.

If you are a firm that does transactional data-- credit card transactions, credit card data, you process and accept credit cards for payment-- PCI, although not a law but a policy, a set of rules and standards, that also dictates a mandate of having a written response plan. And then if you fall into any certain ISO standards-- the ones in particular 17799 or 27002 if that were to apply-- that's also something to be mindful of.

And don't lose sight that some state information security laws may apply to you. The most stringent of the state laws would be Massachusetts. They have a law known as MA 201. Their law, if your business resides in Massachusetts, for example, you're required to maintain a Written Information Security Plan or a WISP as they call it. This type of plan would satisfy that requirement. So, a few things are out there legally that you obviously want to be mindful of to make sure you're meeting compliance there. But, yes, even without a law in place, having a plan is certainly sound advice.

DAN BUELOW: So, Carter has mentioned you have some real-life experience with cyber-attack on your firm. And can you share a bit about this experience and your efforts in developing a cyber incident response plan following this incident?

CARTER BOARDMAN: Yes, Dan. So, what happened-- this would have been back in December of 2020-- we were actually having COVID discontinuity meetings with our senior management. And, of course, COVID had been going on for almost a year. We felt we had a pretty good handle on it for the company.

And then the CEO of our company said, what really started to worry me is cyber. All the meetings I go to, cyber and all these ransomware attacks. So, he tasked myself and our vice president of our IT department go and do some research and find out what we need to do to prepare Merrick in case we get attacked. Because what he said was, I don't want to get into a room, and then we're all pointing fingers. What do we do if something happens?

So, I actually have Beazley as my cyber insurance. But I never really looked at the policy. I looked at the policy. And then I noticed they have a really nice website. So, I looked at the website. And, oh, my gosh. It was full of so much good information. And there was all this stuff.

And then that's the first time I ever saw a cyber response plan, that that's what you needed. Beazley actually has some samples that you can use. They didn't really work for A&E world. So, I knew I needed a plan.

So, the IT VP and myself, we started doing some research. We used an audit company called Plante Moran, which is quite large. And we went to Plante Moran to see if they had a department that does that. And they did. Anyway, we did go with Plante Moran to help us put our plan together.

What was really interesting was this started mid-December. And we're getting ready about the 1st of January or the middle of January. And come to find out we'd actually been hacked back right about the time we started this process in mid-December. We had a bad actor come in, got into our emails, and actually spent a few weeks and knew who the players were and sent an email to our accounting department for one of our larger vendors to change the bank account. And so, we actually made a payment of $165,000 to the wrong bank.

So, we get contacted about a week later saying, hey, where's our payment? We made the payment to the new banking information. We don't have a new bank. So, then we found out we had a problem.

Ironically enough too, I just had a meeting set up that Friday to talk with Beazley to find out more about their services for our research. And we found out we got hit. So that meeting became a little more entailed. And what we thought was interesting was I'm freaking out because we've been hacked. My IT VP, he's freaking out we got hacked.

But then we're talking to the players at Beazley, and they're just very calm because this happens all the time. And they knew just what we needed to do. And they point us the right direction. What's great about their policy-- and I'm really not here to hawk how you should go with Beazley. But I got to tell you, their incident response group is phenomenal. And they have a whole list of providers that you can go to. Before this, before I knew that we had this meeting, we thought we had to go find our own providers.

So, we had talked. We have CrowdStrike. We talked to CrowdStrike. And they go, oh, yeah. We'll put you on the first tier of our list in case you have a response. But you got to pay us $40,000 a year to be on this list. And if you don't spend it, we'll give you other services.

And so, we thought we had to shell out some money. Then we have this meeting with Beazley and find out that, no, you have the policy. You already have first tier with all these providers. And there's a whole selection of providers.

First thing we did was we needed to get a law firm to help us to navigate through all that's going on. And we actually chose Polsinelli, really impressed with them. We used mostly out of New York and Chicago. And we talked to them too. Again, we're nervous. And they're going, oh, no, no. This is not a big deal. We got you covered.

And ours was an email hack. And so, we talked about the other providers for doing the forensics. And they go, well, we're going to give you a couple. We recommend Charles River Associates. They really understand email. Or you can use another company.

And we went with Charles River Associates. Again, we got talking. That same day, they're already starting on the process. RIG had already shut down everything, but they'd already started the process to start doing the forensics.

So, I got to tell you, understanding that we had a law firm to protect us legally to give us advice, now we have a company that come and do the forensics that's going to be in [INAUDIBLE] best interests. It was already at my fingertips, and I didn't know it. So that started the whole process. And then we started preparing our cyber response plan going in conjunction with it. We have an incident, right?

And like I said, we used Plante Moran. Very pragmatic. We like their approach. I like what Alex says. How big should your plan be? Ours is 20 pages. That includes appendices. It's just about the right size.

And what's interesting is my CEO requires that we carry our plans with us in our briefcases or backpacks every day because you don't want to leave it online. You don't know if you're going to be able to access it or not. So, I carry my plan with me because I could be on a business trip, and we've been attacked, and we need to address the issue. I'm actually the incident response manager, so I run the meetings and so forth.

And we have a team that we put together that's our senior management. Basically, we're the ones that address these issues. Merrick's about an 850-person firm in 25 offices. We're large, but we're not super large because a lot of people think your plan should be with your mid-management. And it may be in a very large firm. For us, it really is the top tier management's addressing the issue. And that's how we took care of things.

So, we were starting the process before we got hacked. And that just pushed this forward to go a little quicker. And everything went really well. Of course, near the end, we did have some information, some old emails that may have been seen that had a lot of our stockholder information with birth dates and Social Security numbers and driver's license numbers. So, we got a company called Kroll. They also were provided through Beazley. Kroll specialized in that piece of doing the notifications and having the credit check service with Experian. And so, they took care of all that for us.

And so even though we did our research, and we didn't think they hacked into these emails from the research that was done by CRA, we chose Merrick to be on the side of caution. And so, we notified about 4,000 employees and past employees-- this was really old data-- and gave them the service. And it went really well.

The other good thing was we found out when you had to notify your employees, you have to look at every state that your employee-- we have employees all over the country. And certain states require certain notifications. Well, that's very daunting. But with Polsinelli, it wasn't. They know what they are.

So, we told the states we had employees in. They took care of handling the notification to those attorney generals for those states. And like they told us; you won't get any feedback. And we didn't because it was a small breach considering it wasn't millions of people. But that was really nice to take care of.

So, for being a very stressful time, being hacked, and you just feel violated really. Working with Beazley and all their partners, it really put your mind at ease to know we were taken care of. So that's probably more than you want to know, Dan. But that's kind of how--

DAN BUELOW: No, I think that's great. Again, having somebody here that's lived this, a design professional risk manager-- I think that you touched on a lot there. I think one of the things you certainly touched on is what is the standard of care now within the design profession? It certainly has evolved recently around just this issue around cyber as you pointed out with your particular issue. We've seen other claims against other firms where the payment application process was usually just, hey, sign off that, yeah, this work was completed. But now you better be looking at the fine print of where's that money being transferred to, right?

And to Alex, your point here, and I think Carter touched on it too here is that it's a non-IT plan. You're really talking about what's the stakeholder's plan. And, Alex, and you both really mentioned earlier and throughout this about organizing by sections. Alex, can you talk a little bit about that, what you mean an overview of organizing by sections of this plan?

ALEX RICARDO: Yeah. I mean, very much even as Carter pointed out, it's a stressful moment when you discover you as an organization have succumbed to this type of incident. And although you're going to have very seasoned senior executives all gathered, they're A types. They're all on the A-list. They're definitely going to be very well prepared if you will to deal with the incident.

It's interesting to see when they gather into that situation room, that boardroom, everyone is a little bit like deer in headlights. There's a little bit of panic, a little bit of anxiety. And so, having that type of plan really available, it just helps ease some of that anxiety and makes the process of the investigation go a lot smoother.

So very much, Dan, to your point, you want to have that plan be succinct and organized by sections is really important. You don't have to go and get into the granularity and create 20, 30 sections or what have you. I generally try to keep it to about three or four. You want to have a simple background section. Just describe very briefly what's the purpose of this plan, why do you have it in place.

Keep track of versioning. As I said earlier, it's a living, breathing document. So, every time you update the plan, let's keep a manifest that, hey, what was updated in this version, in the latest version, and so on.

Much like Carter described, he's the incident response manager. He took it on himself to be the custodian of this plan. You want to identify who that is. Just know who owns the plan, who owns the responsibility to keep it current, keep it up to date. That's what you just see in the background.

The second section in my opinion is probably the most critical. You want to define who is the incident response team. So, there are a variety of team members. The most important clearly are the internal members. So, within your organization, you've got to identify who's part of your response team.

And remember, everyone on that team doesn't mean everyone is getting called into or assembled for every incident. It's as the context of the incident is identified, you're going to pull in certain members. So, you're going to likely have risk management, someone from legal, definitely representation from IT and information security.

But maybe you have somebody from HR. Well, why would you have someone of HR part of a cyber incident? Well, what if you had an incident that involved a rogue employee or, as Carter pointed out, it involved employee data? So clearly, someone in HR is going to be part of that incident. So, what let's identify who that person should be if we need to call them into this incident.

So those are the internal members. Guess what? There's external members as well. So very much as Carter pointed out, if you have a cyber insurance provider and a cyber insurance carrier, they're an external member of your response team. Your insurance broker most certainly is going to be part of your external response team.

And then privacy counsel, a forensics firm, if you needed a crisis management firm. Heaven forbid you had a ransomware matter. You're likely going to need a ransom negotiating and payment facilitation firm. The list goes on. But having those folks identified in your plan is just going to make it that much easier when something does happen.

And then there's going to be a section on just managing the incident. Now, clearly, I can give you a full laundry list. We'll be here till tomorrow. But what I try to advise clients in doing when they formulate this type of plan, you're not creating a recipe book. So, you're not creating step one, step two, step three. But rather, let's formulate and assemble a list of questions or checklist items that your team that you've assembled are going to remember they have to deal with and address.

So simple questions like do we need a privacy counsel firm? Is there an insurance carrier we need to notify? Do we need a forensics firm? Is the data involved in our system or a third-party system like a cloud provider?

I would have assembled a series of these questions so as the team has assembled, it becomes your agenda for those meetings. These are the items you're going to have to address and making sure you don't forget to address them. That to me is going to be much more effective than trying to conceivably create that recipe book. And that then becomes a much more useful document.

So those are the key sections. The last section to be honest is a mitigation and remediation section. So clearly, once the dust has settled, what do we have to do to make sure we don't have this type of risk occur again? What are the remediation steps we need to go through?

And in my humble opinion, the most important step is the very last page probably in your plan, which is now that we've finished this risk or this incident, what can we do to improve our plan for the next event? While it's fresh in everybody's head, this is the ideal time to update your plan accordingly to what worked, what didn't work from the event that you just went through. Those are fundamentally the kinds of sections I often try to recommend clients consider when they're crafting and building out this plan.

DAN BUELOW: Excellent advice. And part of that is also getting your staff in sync on what this risk is and understanding how to really avoid allowing your firm to be attacked if you will. And there are certain mitigation steps. And then I know one of the exercises we talk about is this tabletop exercise in that. And, Carter, I know that that's something that you and your firm went through. And if you could tell us a little bit about what is this tabletop exercise, what do we mean by that, and has that been useful for you and your firm?

CARTER BOARDMAN: Yeah, Dan. So just like Alex said, you have an incident, you find out how you could tweak your plan. Well, we did our first tabletop exercise. And we ended up tweaking our plan because you're using your plan as part of the exercise.

So, our plan right now for the company is to have a tabletop every six months. It may not be every six months, but it's within that six to nine months' time frame, we want to have tabletop exercise. I work with Plante Moran. They're the ones right now that are planning those. We talk about what we want to do. The first one we did was--

DAN BUELOW: And, Carter, sorry. But how would you describe to begin with what is a tabletop plan?

CARTER BOARDMAN: Oh, OK. So, tabletop exercise is just they give a scenario that basically they'll go through a scenario that you've been hacked. Our first was more minor. We didn't start with a ransomware, right? We're going to build on ours. Ours was a phishing exercise.

But they'll go through, and they'll say, this just happened. What are you going to do? And then everybody's in the room, everybody that's on the committee. And they all have jobs they've got to do.

So, what are you going to do? Well, I'm going to do this. I'm going to do that. IT's going to check this out. Risk management's going to do this. Legal's going to do that. We're going to call Polsinelli, talk to them and find out what our next step's going to be.

And then they said, OK, then this happened. So then usually they'll throw out another wrinkle that you got to deal with. And we had three of those that happened during the process that we had to change. And then part of ours was is that part of the committee, they're not here in the room. They're traveling. So, we're trying to set up a Teams meeting so we can get them involved or whatever. So, it's trying to keep it as realistic as possible and how would you address that problem at the time it happened.

DAN BUELOW: So, it's a fire drill, if you will, and then how you're going to take the plan that you have in place and execute it essentially with the various scenarios.

CARTER BOARDMAN: Exactly. And then we have a post-meeting to talk about what did we learn. Where do we have some gaps that we need to correct? And so, you put some action item list together to fix those. And then like I said, we went back, and we tweaked our plan.

And then we got another one coming up here in a few weeks. And we're going to escalate. It's going to be a little more in depth, that one. And then we'll go through the same process again. And we'll see where our gaps are, and we'll improve our plan.

DAN BUELOW: It sounds like good advice. [LAUGHS] It sounds like a great exercise. And again, having something in place and then practicing it, if you will. As discussed throughout this, it's really critical that every business not only have the right controls in place to mitigate and manage their cyber liability exposures but to also have a plan in place to respond to any incident. Any firm that has ever had a cyber related claim will tell you that it can be an arduous and very different claim process to get through.

A significant risk to the firm, of course, is the interruption of their business practice. Quantifying this business interruption damages for a service firm can be very difficult. You're not making widgets. And it's not easy as counting how many hours your systems were impaired. And a lot has to go into this.

And we've talked a lot about Beazley, and there's been some great shout outs for Beazley. And deservedly so. There're carriers out there. The good carriers out there should have resources available and should work with you together with your broker that should have specialists in this area as well.

Alex, can you just tell us a little bit, talk to us a little bit about an overview and what is the business interruption loss and the proof of loss process that firms just need to be aware of? Obviously, we could spend a whole other podcast just on the forensic accounting and everything else that goes into this. But just an overview on that, the proof of loss process and the business interruption.

ALEX RICARDO: It's definitely an important coverage because it definitely will cover financial losses that a company may face as an indirect loss, if you will, from a cyber incident. So, Carter, of course, gave an excellent example that his organization went through with the losses around the sensitive data that his company owned. And that's definitely a direct loss that clearly needs to be addressed under the policy.

But there are also what I would often just call the indirect losses. And we don't think about what those losses are until we actually start to actually calculate them. So, when we think about a business interruption loss, there is additional losses that occur that that attacker, that threat actor, in addition to stealing data in this example that could have crippled the workings of an organization from succeeding and proceeding in earning income.

Now, this goes very much, Dan, to the point you mentioned earlier where you're going to need resources on how do we calculate that income loss. That's where the forensics accounting firms come into play. Their expertise is to get it all into the minutia and the granularity of determining how many employees does the firm have, what's the hourly wages, what's the historical revenue this organization may have brought in during this time period where the business was interrupted, and so on. They go through all of that calculus to help try and get some kind of measure of number, a quantifiable number of where income the company was lost due to the cyber incident itself.

Then there are going to be expenditures to do that calculus. And so forensic accounting firms, different forensics firms even on the IT front are going to have to be an expenditure to compute this. And then there are other additional expenses that may come out of it where, in some instances, you have to recreate data. So, there's what's known as data recreation expenditures. Maybe certain data not only was stolen, but maybe some of it got corrupt or got erased or got destroyed in the process by the threat actor. And so, there's data recreation efforts and expenditures that need to come into play.

DAN BUELOW: Yeah. And again, I think you did a nice job illustrating the importance of having these plans in place, right? I mean, at the end of the day, what we want to do is to reduce that time where you're going to be impacted as a business and ideally mitigate it on the front end with good sound risk management practices. So, I want to thank Carter. Carter, thank you for joining us on this. This was excellent, Carter Boardman.

CARTER BOARDMAN: Thank you, Dan. Appreciate it.

DAN BUELOW: Really appreciate you sharing your experience and expertise on this. And, Alex Ricardo, thank you again.

ALEX RICARDO: Yeah, no. My pleasure, Dan. Always a pleasure to work with you.

DAN BUELOW: And thank you for joining us for another Talk to Me About A&E podcast. Talk to you soon.

SPEAKER: 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. The information contained herein is not intended to constitute legal or other professional advice and should not be relied upon in lieu of consultation with your own legal advisors.

In the event you would like more information regarding your insurance coverage, please do not hesitate to reach out to us. In North America, WTW offers insurance products through licensed entities including Willis Towers Watson Northeast Incorporated in the United States and Willis Canada Incorporated in Canada.

[MUSIC PLAYING]