Talk to Me About A&E: Episode 22 — Cyber risk alert: Fraudulent funds transfer

[MUSIC PLAYING]

TARA ALBIN: One thing very important is lacking cybersecurity training within companies. That is something that the underwriters always ask about.

SPEAKER 1: 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. I'm Dan Buelow, and today we will be sharing some cyber claim stories around some recent cyber claim trends evolving design professional firms.

Our Willis A&E group with the help of our WTW cyber team has produced quite a bit of material on cyber-related materials including podcasts, technical briefs, on-demand webinars, and quarterly market realities reports. We've done this because of the significant volatility and uncertainty within the cyber liability marketplace. Our goal is to help design firms and their IT consultants stay abreast of what's happening in the cyber liability marketplace, and more importantly, what firms should be doing to mitigate this risk.

And we've added all these materials to a folder that can be found in the Education Center of our Willis A&E website, which can be found at www.wtwae.com. So if you haven't checked that out, I would suggest you do, as there's a lot of great information available, compliments of Willis A&E.

I wasn't really planning on doing another cyber-related podcast. However, we've been seeing an alarming number of cyber-related claims recently involving fraudulent transfer of funds and rogue employees. In fact, we've had two such claims come up very recently.

The first was a claim from an architect that approved a payment application. This firm was issued a payment request, which was identical to the last payment request except that it had reflected an update in the work that had been done and contained payment instructions that directed half a million dollars to be deposited in some cyber criminal's bank account. Apparently, this cyber criminal had been monitoring the firm's correspondences and was able to update the work progress on this payment application.

What is the standard of care of a design professional now when it comes to this? What can firms do to mitigate this from happening? As you can imagine, there was a lot of back and forth as to whose fault this was, and it was really a real strain on the relationship between the owner and the architect in this case.

The second matter, an employee of a design firm downloaded project files without permission, which was a real problem in that this was a very high-profile project with an NDA in place. This was very sensitive information, and again, raises a lot of questions, including how to mitigate this risk.

So this is just a couple of examples, but I thought it'd be a great idea to bring in a couple of professionals to help us talk through this and maybe give us some more examples on this. And so with me today, I have two members of our WTW cyber team to share some stories and some expertise and information on this. And I'd like you to welcome Tara Albin and Liz Caldwell. Hello, Tara and Liz.

TARA ALBIN: Hi, Dan. Thanks for having us.

DAN BUELOW: Great to have you here. Liz, how are you doing?

ELIZABETH CALDWELL: Excellent. Happy to be here today.

DAN BUELOW: All right. Our Willis A&E team is very fortunate to have access to the WTW cyber team, which is a specialty division dedicated to placing cyber coverage and managing cyber risk. Let me tell you a little bit about our two guests here today.

So Tara is the Midwest Region Cyber Leader and Senior Placement Cyber Specialist for the WTW cyber group. Using her expertise in cyber liability coverage, Tara educates clients in their risks, exposures, and assists in placing the appropriate coverage that specifically fits the client's needs with her broad knowledge and utilization of a lot of great information that we have and tools within WTW. So Tara, thanks for joining us.

And Liz is a cyber claims leader for WTW's cyber group. And in this role, Liz advocates on behalf of the WTW clients on cyber-related claims. And prior to joining WTW, Liz was with Chubb's Office of General Counsel as Cyber E&O Counsel where she supported the cyber E&O business in its day-to-day activities and in developing new products.

And prior to that, Liz was with AIG where she handled cyber claims. Liz earned her law degree from Tulane University Law School and is admitted in the New York State Bar. So thank you both for joining us.
Tara, maybe we can start with you, and then Liz can give us some background and some claims stories and input on all this. So as mentioned, our group has seen a lot of claims involving design professionals, and there has been a disturbing trend involving fraudulent fund transfer. Can you talk to us about this trend? How do these particular issues originate? And what are some tactics used by these bad actors that companies should be looking for?

TARA ALBIN: Thanks, Dan. So not just A&E companies, but we see this trend also on the construction side. So any time companies have service providers, there's a lot of payments going back and forth for services and goods, et cetera, we tend to see this heightened trend.

Some of the reasons behind it may be a firm or a service provider has had a prior cyber event. Although forensics come in and kind of do an evaluation of the system, sometimes they're not always fully out. I mean, they can linger at times or get just enough information to use at a later date.

Another thing we see too, in most companies we are seeing a lot of M&A activity. So if there is a hacker sitting undetected in a network, they're kind of monitoring, just sitting there quietly undetected, monitoring M&A activity, they know there's something ready to be closed on. And they may sit there and pounce at the right time and send a very legitimate-looking email about quickly transferring funds. Looks all on the up and up at the time, but with a little deeper digging and kind of some secondary steps in place, it can be prevented.

DAN BUELOW: And what are some of the consequences as a result of fraudulent funds transfer or invoice manipulation?

TARA ALBIN: Yeah. So some of the consequences with this is not being able to recover funds or some of the goods that would be applicable to invoice manipulation with the goods. Unexpected costs and expenses incurred. This is money's gone out of the door. The goods have gone out of the door. Now we've got to recover them. So unnecessary costs and expenses involved.

And importantly, reputational harm. If others find out about this, word gets around, it may tarnish the company's reputation that you're a little sloppy with paying funds or something along those lines. And lost business, frankly. I mean, what if it got out that this happened a couple of times and then companies start not really trusting you to do business with?

DAN BUELOW: There's a real question again, as I mentioned. What is the standard of care now? As a design professional in this scenario, the design professional's been approving payment applications from the beginning of time. And what they're basically being asked to do is, hey, did the contractor do this work, and should we pay this invoice?

Now they're being asked to double check, if you will, if it's valid fund transfer instructions or whatever else to look at. What is the standard of care? And I could see how there could be a lot of finger pointing here. But nobody's going to be happy because a lot of money went to the wrong spot.

TARA ALBIN: What I can recommend, limiting the amount of people that are allowed to authorize these payments and transactions. Limit it to just maybe one or two people, and then have an escalation process in place, several steps. If it is under $10,000 in a payment, there's a certain protocol to follow. If it's between $10,000 and $25,000-- and it kind of goes up like that. And then maybe if it's over $100,000, it gets escalated to the CFO for sign-off, or something along those lines. And really keeping that line of authority for payments very tight.

And having secondary procedures in place, things like clawback provisions. In a former work life when you could walk down the hall and knock on the door of somebody-- of the CFO's office and just say, hey, I received this. Is this legitimate? Can I authorize it? Now with the remote workforce that's been a little bit challenging, but it does seem that some companies are going back into the office. So really, that face-to-face authorization.

And picking up the phone. Don't just do everything in email, because remember, you could have a hacker monitoring your emails and sitting there and watching. So just making sure those extra safety steps are in place. I don't know, Liz, if you have anything to add to that from what you've seen.

ELIZABETH CALDWELL: No, I absolutely agree. Having different people involved in the process, not just one person responsible for approving payments and having an escalation process, I definitely think that's a best practice that companies should incorporate into their privacy policies or policies in general for processing payments.

DAN BUELOW: Yeah, and you mentioned picking up the phone. And in this day and age, it seems like everybody's a little reluctant to do that. But it seems like it could save a lot of time by doing just that, right? I mean, if you have one of these claims happen or these issues come up, you're going to be spending a lot of time on it, so I don't think it's all that inefficient to pick up the phone and confirm some of these authorizations as well, right?

TARA ALBIN: Mm-hmm. Something that just occurred to me too, a very basic way of hackers convincing people to make these payments is LinkedIn. We're all very free with what we put about ourselves on LinkedIn, what departments we work in, what we do. And hackers love to scan through LinkedIn and pick a person.

And another tool to think about is having that external email flag. So sometimes when those emails come from the outside, it's flagged as being an external email rather than if it comes from the inside, it really looks legitimate. So there's tools out there that can assist when employees receive those external emails requiring payment, things along those lines. But yeah, we see hackers also scanning LinkedIn and using that to their advantage.

DAN BUELOW: That's a good point. So Liz, can you give us a couple of claims stories here, some scary stories involving fraudulent fund transfer?

ELIZABETH CALDWELL: Absolutely. Yeah. I've got a couple of scenarios to share. One type of claims scenario we see quite a bit is situations where a client actually receives a fraudulent instruction and then makes payment to the bad actor.

So one example I'd like to share is where an insured suffered a business email compromise incident where a bad actor gained unauthorized access to an employee's corporate email account. The bad actor then caused fictitious emails to be sent out to the insurance customers, requesting that they make any future payments to a new bank account that unfortunately belonged to the bad actor and not the insured.

So as a result of this email, one of the insured's customers ended up making a payment to the fraudulent bank account in the amount of around $100,000. Since this occurred, the customer has spoken with the bank. They're trying to see if they can recover any funds, which I don't believe they have yet, unfortunately. And interestingly, the insured believes that this business email compromise incident actually results from a prior ransomware incident that they experienced a few weeks back.

So in terms of coverage for this incident, something the client should be aware of is that some cyber insurers provide coverage for funds that the insured should have been paid by a client or that a client ends up paying, whereas others don't. So it's very important to see how your cyber policies, cybercrime, insuring agreements, how broad they are, what types of coverage they provide.

But in this specific circumstance, the insured's cybercrime endorsement did provide coverage for invoice manipulation fraud, which is where the insured-- or I guess their system is compromised, and then fraudulent payment instructions are released to customers as a result of a security breach. So fortunately here, there is coverage. But it's possible in some circumstances that the cybercrime language isn't this broad. So certainly something for people to be on the lookout for.

DAN BUELOW: Yeah, a couple of good points there is making sure what's in your policy, and understanding that these coverages can and will evolve, right? We've seen these coverages come in. We've seen some of them excluded. We've seen dropdown limits on some of this available coverage, so that's an important point.
And also, there is a separate product out there, a crime policy that some firms I know have also purchased to kind of belt suspender or have some additional coverage on this. But all of this is kind of secondary, isn't it, to some robust business practices and IT practices around what to do to mitigate it? Give us another one, Liz. You've got another story for us?

ELIZABETH CALDWELL: Absolutely. Yes, so another circumstance that we had was a situation where an employee of the insured had their work email account accessed by a bad actor. And as a result, false wire instructions were sent from the employee's email account to their financial advisor. And then as a result, the financial advisor transferred funds from the employee's personal bank account to the bad actor.

Interestingly, this was a situation where it wasn't the insured's funds that were compromised, but it was the employee's. And unfortunately in this circumstance, there was not coverage because the cybercrime insuring agreement really provides coverage for situations where it's money that's transferred from the insured's corporate bank account and not an employee's personal funds. So this was an unfortunate circumstance.

But I believe I have seen in a few limited instances endorsements to cyber policies where there may be coverage for situations where a C-suite member's email account is compromised, and then they have funds lost from their personal account. But again, that's more the exception than the rule, and there has to be a specific endorsement for that type of coverage.

DAN BUELOW: OK. And you have one more for us, I see.

ELIZABETH CALDWELL: I do. The next one is a really common type of scenario we see quite a bit, basically where the insured themselves make payment to a bad actor who's purporting to be one of their normal vendors. An example is where a bad actor sends emails to the insured with an email address that's just a little bit off from the normal email address, like one letter is switched or something.

And then in this email, the bad actor provided a document appearing to be on bank letterhead that contained revised bank account information. And the insured ultimately made the changes to the account information and made a regularly scheduled payment to this vendor in the amount of $200,000. But of course, the payment went to the bad actor and not the vendor.

Once the insured discovered that this incident had occurred, they tried to contact the bank to have the payments recalled, and they also filed an Internet Crime Complaint with the FBI, which is something that we always recommend that insureds do after an incident, particularly since some policies require reporting within 48 hours of discovery of the incident. So always a best practice to report to the FBI IC3 unit.

Luckily, this type of incident is typically covered under cybercrime insuring agreements, social engineering coverage, since it is the insured who received a fraudulent instruction and then transferred funds from their corporate account. So kind of the run-of-the-mill type of funds transfer fraud, social engineering claim that we see.

DAN BUELOW: So those are three great examples. And again, I think some of the advice that you and Tara gave on what to do to mitigate this, what practices to have in place-- and firms really do need to have an incident response plan in place, don't they, for these different cyber-related matters? Because they often happen in inopportune times, and you need to think about, who are the stakeholders within your business that may be impacted and/or have responsibility?

You know, who to call? As you mentioned, call the FBI. But you really do want to get a hold of your insurance carrier and to know who to call and what to do in the event of one of these claims or these issues.

ELIZABETH CALDWELL: Absolutely. Yeah, knowing who your carriers are. If you have a crime policy, having that information handy as well for any funds transfer-type matters. But definitely, yeah, making sure that all stakeholders are aware of the reporting process, what steps to take. That certainly makes a difference if these types of incidents do occur.

DAN BUELOW: All right. So that's some good examples around fraudulent fund transfer here. The next up I want to talk a little bit here would be on rogue employees. Tara, you want to talk a little bit about what we mean by a rogue employee and some of the issues to consider specific to that?

TARA ALBIN: Yeah, for sure. So a rogue employee sounds negative. Sometimes these can just be complete innocent mistakes. But at the end of it, there's a cyber event that has taken place as a result.

But in this current economic environment, people are hurting for money and can't pay their bills. So sometimes it's just a monetary motivation that they may go rogue and do something against company policy to make some money, whether it's stealing proprietary information, downloading files, working with a third party just for money.

Also, everybody's working twice as hard lately and don't feel that they're being fully compensated. Or it's just a general toxic workplace. That's not good for employees. They don't feel happy in their jobs. They don't feel motivated to do a good job. And then it becomes sloppy, right? And all of these things can cause a cyber event.

One thing very important is lacking cybersecurity training within companies. That is something that the underwriters always ask about. Not only is it in place, but how often is it offered?

And just training employees how important it is to be on the alert. When you get an email that doesn't quite look right with a link or an attachment, just knowing to not open it, not click on the link. And escalate it to IT or whoever their escalation process involves, because employees continue to be the weakest link when it comes to cyber events. So those handful of examples is something to think about, especially cybersecurity training.

DAN BUELOW: And to your point, it's not often a criminal act, if you will, or a nefarious act. It can be a training issue or just not understanding responsibilities and so forth. The example I gave earlier around downloading project files, this was nothing that was, again, intentional to bring harm to the firm. This employee was wanting to essentially update their own resume, if you will, I think essentially was what they were looking to do. But they shouldn't have done it.

And without talking through these things, like you said, to have some of this training with employees, not only how to catch some of these things early on that are phishing incidences or whatever, but also to talk about the standard of care the, fact that we do have nondisclosure agreements out there with other clients and so forth, just to understand that.

And then the question back to you on this, Tara, too is, what can firms do, again, to monitor or mitigate this? I would think that one thing would be just to keep an eye on unusual activity around downloading of files, right? I'm sure there's ways of tracking that.

TARA ALBIN: Yeah. I mean, what I would recommend is not allowing personal devices to be used, not allowing anything to be downloaded, especially to thumb drives or whatever other device or storage device to use. But using company-issued equipment, encrypting data, and just not allowing those downloads to take place. Or having very strict protocols in place if it's absolutely necessary to download something.

DAN BUELOW: Great points. And Liz, you have a couple of claim examples for us specific to rogue employees?

ELIZABETH CALDWELL: Specific to rogue employees, yeah. One example that we've seen is situations where an independent contractor actually stored electronic PII from a company-issued thumb drive onto their personal Google Drive without any sort of business associate agreement. So this did lead to a potential compromise of protected information.

There is coverage for these types of matters under a first-party breach response, ensuring agreements of cyber policy. So cost to notify the individuals whose protected information was compromised. But at the end of the day, it's an unfortunate incident that really could have been prevented and it's-- yeah, just something that happens sometimes. Another type of incident we've seen is, yeah, situations where an employee will access client data or, again, PII without any sort of business justification.

DAN BUELOW: Yeah. And again, to talk to your staff and educate your staff as to what's acceptable or not, and to have training. And I know even around phishing, we've talked about-- I think this kind of next segment we're going to talk a little bit is around ransomware and such.

But tabletop exercises or whatever else to Tara's point is that these underwriters are really asking-- there's a lot more scrutiny around what firms are doing to have these precautionary measures and training in place, right? And so everything is important when it comes to educating your staff.

So we've done some past programs focusing on ransomware. Is there still a major risk, Tara, that firms need to address? And any updates that you can provide specific to ransomware?

TARA ALBIN: Yeah, for sure. So again, critical staff are trained, because a lot of times that's how the hackers are getting in, by employees clicking on links, and that's how the malware gets in.

But yeah, ransomware. I'm sure many of you have read articles, especially on LinkedIn, that ransomware is on the decline. It's dropping off. That's giving people, I feel, a false sense of, oh, we're good. It's not going away. Yes, it has slowed down and ransom payments-- so companies paying a ransom has declined slightly. That can be attributed to better controls being put in place and companies being able to recover on their own and not having to pay a ransom, which is good.

But the slowdown is temporary. Much of what we're hearing, particularly from our threat intelligence side of the house, is a lot with the ongoing war in Ukraine. Many of those hacking groups have had to redirect manpower and funds to fight the war. So there's a slowdown, particularly from Russia and Ukraine, on ransomware events, and that is somewhat behind it.

So there's a slowdown, but everything I hear and read is this is very temporary. So there's not a false sense of security. Still guards are very much up. And just don't take a breath and sit back, because it will be back. Liz, do you have-- from the claims side, have you witnessed anything else?

ELIZABETH CALDWELL: No. I mean, there's definitely been a decreased number in the amount of ransomware incidents we've been seeing, but that doesn't mean that the ones that we have been seeing aren't still of a high severity or aren't resulting in significant business interruption loss. So even if the frequency is down, it's still something that all types of companies really need to be aware of and kind of prepare for if it happens. So I still think it's certainly a threat even if it's a bit less prevalent than it was, say, a year or a year and a half ago.

DAN BUELOW: I would agree, Tara, on your point that I think probably the controls that have been required by these underwriters now that firms need to have in place in order even to be offered insurance these days. But also that you really need to be working with your underwriters and your broker early on in the process to get a clear understanding of what those updated controls are, right? Because this will evolve, and these criminals will continue to come up with some new tricks, if you will, I'm sure. So I think those are all some good points here. Liz, you want to bring us home with a claims story or two involving ransomware?

ELIZABETH CALDWELL: Sure, absolutely. So I guess the most common type of situation we see is where an insured suffers a ransomware attack. It ends up resulting in a company-wide outage. And as a result, the insured really isn't able to go forth with its day-to-day business, and they end up suffering lost income.

So we've seen situations where the insured will have to pay the ransom, or they may not have to because they have backups. But you know, irrespective of whether the ransom amount is paid, just the business interruption loss as a result of the shutdown tends to be where a lot of the exposure is. Particularly now that people are starting to have more backups and aren't paying ransoms, they're still suffering the BI loss, potentially.

DAN BUELOW: Well, thanks, Liz. Those are a couple of good examples here, and it's always great to hear some claims stories. Tara, Liz, any parting words of wisdom or advice or thoughts on our topic today?

TARA ALBIN: Yeah, I'm happy to address that. I would just recommend clients see what's available within your policy, because many of these insurance carriers do provide pre-breach services, or they may have a portal with various templates or recommendations. So if you're not sure, look at your policy. Ask your broker. See what's available to you. Take advantage of those, because sometimes these services can be either discounted or free, and you can get some further guidance. And of course, here at WTW, we also have a team of cyber risk consultants for added services too.

DAN BUELOW: No, that's a great point. And again, some of these carriers really have invested quite a bit and have a lot of materials and information on their websites and so forth available. That's a very good point. Liz?

ELIZABETH CALDWELL: As a parting thought, I would really echo what Tara said. Reviewing your policy, really understanding what types of coverages you have. Certainly making sure that you have a cybercrime endorsement or ensuring agreements added to your policy since a lot of times that is added via endorsement and isn't automatically baked into your cyber policy.

I gave an example of a situation where an insured was owed funds from a client. So seeing whether your specific cybercrime coverages would provide coverage for that type of situation where you lose out on money that you're owed from a client as a result of a social engineering incident. So just speaking with your broker, making sure that you're comfortable, that you have the cybercrime coverage you need. And of course, looking into having a standalone crime policy as well that can pick up coverage that may be not in certain cybercrime insuring agreements.

DAN BUELOW: Excellent points. And Liz, you can speak firsthand on this point, though, but getting through a cyber claim can be a difficult and painful process. True or false? [LAUGHS]

ELIZABETH CALDWELL: Absolutely. It can be very lengthy, particularly if there is a business interruption component. But at WTW, the claims advocacy group are certainly here to assist throughout the claims process and try to guide you through it in as painless of a way as possible. But it can certainly be time-consuming, for sure, specifically-- yeah, with data recovery, business income loss, and all that.

DAN BUELOW: Excellent points. And again, I mean, that's the purpose of this discussion today is to try to help folks mitigate the risk and avoid claims entirely. So there's some best practices I think and some lessons learned from all this.

And I want to thank both Tara and Liz for sharing their expertise and experience with us on this very important topic. We really are fortunate to have dedicated specialists in this area to support our group here. And thanks, again, Tara and Liz. Thank you both.

TARA ALBIN: Thanks, Dan.

ELIZABETH CALDWELL: Thanks, Dan.

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

[MUSIC PLAYING]

SPEAKER 1: 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]