Risk ON AIR

Cyber Series

Transcript

Protect your Legal Practice from Cyber Fraud

Intro

In part one of Lawcover's Cyber Podcast series, host Julian Morrow, talks to Lawcover Chief Legal Officer, Elissa Baxter, about how cyber fraud has evolved over the last few years and what law practices can do to protect themselves and their clients.

Julian: Welcome to Risk On Air. I'm Julian Morrow and today we are talking about the never relaxing topic of cyber assisted fraud. I'm very pleased to say that we're joined by Elissa Baxter, the Chief Legal Officer at Lawcover. Welcome, Elissa.

Elissa: Thank you, it's a pleasure to be here.

Julian: Now, Elissa, when did Lawcover first get a claim from a law practice for loss of client funds due to a cybercrime?

Elissa: So, I think our first claim came through in about 2017. And we were a little surprised that we were really dealing with fraud and that we were then having to cover client funds that were lost out of a law practice's trust account.

Julian: 2017, in some ways seems like a long time ago, but in cybercrime it's an age ago.

What sort of issues were you dealing with in the early days in the cyber area, and how's it changed since then?

Elissa: The very first claims were really quite rudimentary, so it was just an email that had come into the law practice looking like it came in from a client's email address, but that email address had been slightly changed.

Julian: So this is your classic email fraud scam.

Elissa: Indeed, except it wasn't very sophisticated. It was fairly obvious that it wasn't a legit email. It came into the law practice and said I've changed my bank account details; can you please send the money through to this bank? And the lawyer did it, and afterwards it became clear that they'd sent it to the wrong place.

We started getting our messaging out around then that lawyers need to be a little bit more careful, checking that the bank account details sent in an email were legitimate, and we really started ramping up our messaging around that, and we also put in place a group cyber policy for the benefit of all of our insureds.

Since then, lawyers have become a lot better. We actually saw claims drop off quite dramatically in that first couple of years and we thought job done, we've solved the problem.

Julian: If only.

Elissa: Yeah, the criminals had to move to an easier target, because lawyers knew what they were doing by then and were checking bank account details before they paid money out. And so, then the criminals started targeting the clients and sending the fraudulent emails to the clients, and the clients who were less sophisticated would send the money, thinking it was going to the law practice, actually off to a fraudster's bank account. So, we've had to keep evolving our messages and it's changed quite a lot. Now there's quite a few clients who are quite savvy. They do check bank account details and now we're seeing an evolution where the criminals are kind of staying one step ahead of that and fraudulently confirming bank account details with the client or with the law practice and still fooling them into paying their money away.

Julian: And that comes to the broader question of what steps can law firms take to protect their clients' funds from being stolen. But how have the steps that you need to take changed?

Elissa: Yeah, so in the olden days, when I first started practice, almost everything was done over the phone or by letter, and letters took a long time to get there, so you would always do things over the telephone. We evolved into relying on email. It's easy, we're all comfortable with it. You can send an email, someone can get back to you when they're ready, and it's taken a while to educate people that email isn't really secure and to get across the message when anything's got to do with money, you can't really rely on email. We've now got that message across. I think that you need to assume always that an email is going to be intercepted or might've already been intercepted. So people are now picking up the telephone, but what we're also doing is having to get the message out that talking on the telephone sometimes isn't enough. Do you know enough about your client to know that it's your client you're talking to on the telephone? And also, you might need to warn your client that this could be an issue in the future.

People often put a warning in the footer of their email that says cyber scam is a problem, and so you need to check bank account details and tell their clients that. Some people put it in their retainer letters. Some people put in their retainer letters, *"This is the law firm's trust account details. We will never change these details by email."* So, there are a few steps that you can take. I'm going to say probably best practice would be make sure you meet your client. Make sure you meet your client in person, hand them a letter that has in it in hard copy, very old school bank account details, a telephone number that they can call to check, and say we're never going to change those bank account details by email. That way you know for sure that this person has got the information that they need. And then the criminals aren't going to be able to get around that by some kind of scam that they might come up with.

And criminals have been coming up with these pretty extensive scams. We've seen emails come in saying *"I can't check the bank account details over the phone, I have an ear infection"* or *"I'm just about to go overseas and get on a plane, just text me and I will confirm the bank account details by text."* So, people have been trying to get around the personally speaking on the phone. But most recently we've started to see the criminals themselves taking the step of saying I know you want to check bank account details, so

I'm just calling into the office and I'm going to confirm the bank account details with you preemptively. And that is very tricky if you're not speaking to the person who's met the client before.

Most of our staff, the receptionists and the secretaries, they want to be helpful and they want to do their job and they want to help clients and so if a client calls in, they're not going to ask too many questions, they're just going to try and do the right thing. They know they should check bank account details and so when the client's called in, they go, *"oh thank you for doing this, this is fantastic"*. They believe they're being helpful, they believe they're doing their job and they're not quite being suspicious enough to say *"how do I know this is Julian Morrow that I'm speaking to? How do I know that you're not someone else?"* Just asking that extra question.

Julian: You can see how easily that could be just a little crack in the system because different firms have people coming and going, someone might be sick, there might be a temp on and it's actually really hard to maintain that level of client business service but also be cautious and check identities, because I suppose what you're saying is that in the old days we used to be able to trust that a verbal confirmation of some sort was most probably going to be okay. But now impersonation is really a risk in terms of verifying bank account details and the like.

Elissa: Absolutely. And the firms that are most at risk for this kind of thing are firms that have between two and five partners. So, if you've got two and five partners, you've got a couple of staff, you've got some admin staff, some support, so you might have 10 or 15 people in the office. Enough people that there can be miscommunication. We aren't seeing as much business email compromise or fraud in one partner practices or sole practitioners. Most of them know their clients, so if a client calls in, they'll go, *"that doesn't sound like Julian's voice. I'm not certain about this. I'm just going to hang up and call back the number that I know"*. That's where I think we can fall down is where the person who might have the relationship with the client isn't the person taking the phone call. We've got to walk that fine line right between being rude you don't want to be rude to your client but being a little bit suspicious because you need to be careful.

Julian: And it used to be the case that if you heard a voice that you knew, you could trust that that was the person that you were talking to. The technology clearly now exists for artificial intelligence to generate something that sounds like another person's voice. Is that something you've actually seen coming through to cyber assisted fraud claims at Lawcover, or is it something that maybe is on the horizon?

Elissa: I think it's something that's on the horizon. So we haven't seen that happen in the context of claims against solicitors, but I have heard in the insurance context of one very large fraud that happened in the US and it wasn't just artificial intelligence or generating a voice, it was actually generating an image. So, it was like a Teams call where the CEO was on the screen giving instructions to someone who was in another country, but they knew enough, they had interacted enough with the CEO to know what they look like and gave those instructions and the money was paid away. So, I have heard of it happening. I think you need to have a fair bit of source material so, like your voice, probably someone would be able to sample.

Julian: They could take it off the Risk On Air podcast.

Transcript

Protect your Legal Practice from Cyber Fraud

Elissa: Take it off the Risk On Air podcast. But for most people there won't be enough out there in the public domain for that necessarily to be a risk right away. But what I think it can do is, for example, mask accents so you might be getting a fraudster from another country who is making a telephone call and in real time their voice might be being translated to an Australian accent, which might make you more comfortable with accepting bank account details being verified.

Julian: There are just so many levels of things you need to be aware of, but really, from what you're saying, there's a mix of technical tools that you need, but then also the human element as is so often the case in scams, it's the human element which is the critical one, and that means training is important as well.

Elissa: Training not only your staff. It's incredibly important to train your staff, not just your legal staff, your support staff especially because often it's the support staff who are going to be making these phone calls and checking bank account details but also training your clients, getting your clients understanding that they can't necessarily trust everything that is sent in an email. If there's an email that says we've changed our trust account details, the very first thing you think is that must be a scam, because that's where we're seeing most of these scams happen. Any email that talks about money be suspicious about it. So, train all your staff and train your clients, especially to be aware of this kind of thing.

And also, I think we all need to train ourselves to just stop for an extra second and ask the question, *"does this look right?"* Because what we're often seeing with cyber scams is people get things right time and time and time again. And it's the Friday afternoon, it's the week before Christmas, it's in between Christmas and New Year, it's over Easter. That's where people are just kind of flicking off the last email before they're going to go on holiday. That's when the mistakes happen. People get off a plane, they're jet lagged. They look at an email, they click on it. That's where mistakes happen, because people aren't being vigilant all the time. I know it's hard. It's a council of perfection. We can't all be perfect all the time. But just stop for a second and ask the question does this seem suspicious?

Julian: And I suppose we should all assume that every human is going to have a lapse at some point. So systems need to not be vulnerable to a lapse by one human in the chain.

Elissa: Yes, that's exactly right. I mean, humans are going to be the weakest point in any system because every human can make a mistake. So we do need those backup systems around us. But doing double checks, asking the extra question, it might seem rude, but calling the client twice, calling the client on two different numbers, whatever it is that's going to make sure that you've actually got the right information. Maybe making a test payment, so if you've got the client on a Teams meeting, you're confident it really is the client. You know them, you've got them there, you know who they are. Get them to send you a dollar, see if you can see it. Okay, that's come through to the right place. So now you can send your $100,000 or $500,000.

Julian: Sounds very wise. Of course, sometimes things are going to go wrong, and thankfully that's where all Lawcover members can take at least some consolation in the fact that Lawcover does have a Cyber Risk Insurance Policy. Could you tell us about it, Elissa, and what its key benefits are for members?

Elissa: Back in 2017, when we saw that first claim come in, we knew this was going to be a problem, and part of what we do with our risk management education is to tell people the ways in which claims happen against solicitors. We kind of scare them a little bit, but we then try and give them the tools that they can do something about it.

Transcript

Protect your Legal Practice from Cyber Fraud

We knew cyber was going to be a problem, and so we purchased a group policy. Now it's not actually a Lawcover policy. Lawcover is actually the insured in that policy. We bought the policy for the benefit of all of our insured members. So, none of those people have to make an application and they don't have to pay any kind of premium. We bought it on their behalf. It's a relatively low level of cover it's like $50,000, but it's like a basic level of cover. It covers everyone, though. I think the primary benefit of it is it gives you emergency assistance. So, if you think you might've had a cyber breach, if you think you might've had hackers in your system, you can just call up a number and get forensic people in straight away to check your system and make sure everything's okay. That's, I think, the primary benefit of the policy, but it has a few other benefits. It has a couple of other kinds of cover. So, if client funds are stolen or are paid away, they will be covered under the Lawcover Professional Indemnity Policy. If the insured firm's own money is paid out of the office account, that will be covered under the cyber group policy. Breaches of privacy, you might have to notify the privacy commissioner. You might need to notify clients. Those kinds of expenses are going to be covered. If your system is shut down because of a ransomware attack and your system then needs to be rebuilt, the rebuilding costs are covered under that policy and actually the ransom itself.

Now what we hope to do is never to pay a ransom, but if your system is shut down and there is no available backup, every now and again it becomes necessary to pay a ransom. Sometimes they're very small in order to get the system unlocked. Solicitors in particular, find that very difficult if they have a trust account and they don't have access to their trust account details, they can't function and so that's their whole business that's stopped. Business interruption is also covered under the policy. So whatever loss of business you've had for that day when the office was shut down, that will also be covered under the policy, so that cyber group policy only has a $50,000 limit, but it can be accessed in a number of different ways.

Julian: And I've got to say Elissa, over the years when we've been talking on Risk On Air, I have noticed a bit of a trend amongst insurers. They do seem to say that you should get in touch with your insurer if you're concerned about an incident, pretty quickly. Would that happen to apply to the cyber risk insurance policy as well?

Elissa: Absolutely. In fact, that is probably the main thing that people should do. The reason is, if you've had a cyber incident, money's been paid away, if it's been paid to an Australian bank account, that bank, if you contact them quickly enough, can put a stop on the money. Now, often the money's gone overseas almost straight away, but they do have ways of clawing it back. The quicker the bank knows, the better the chances are of clawing that money back. So, we will say to people who do call us on our hotline, we'll get the forensics team in and make sure that there's nothing else happening in your system. Call the bank straight away. See if you can get a stop put on the money.

It's good to call the police and tell them that there's been a crime. There's so much cybercrime that's happening. Unfortunately, the police are not actively investigating a lot of those matters. Nevertheless, you still need to call the police. There's a whole bunch of people that you need to call. If you call us first, we can start that process. We've got a whole checklist of things that we can tell you to do that are going to help you in that circumstance.

Julian: You mentioned that in the early days there was a bit of a spike, but then things tended to ease off a little bit. Is the Cyber Risk Insurance Policy an active area of claims? Is this something that a lot of members are experiencing?

Transcript

Protect your Legal Practice from Cyber Fraud

Elissa: So, it's not our biggest area of claim by any stretch of the imagination, certainly not on the professional indemnity policy, but we're seeing enough claims come in that you can really start to see trends and what we are seeing on the group cyber policy, that is, the emergency response policy, quite a few claims come in where there's no loss of funds, no loss of client funds and what's often happened in those cases is that the solicitor will call us up and say I think I might've been hacked.

And the reason they know they might've been hacked is that a client has received an email saying we've changed our bank account details. The client was educated enough to pick up the phone and call the law firm and say got this email and that seemed weird to me. And they said no, no, that wasn't us, we didn't send that email. They realise there's a problem, they get the forensics team in, it gets sorted out and all they've really done is fix a problem and there's been no loss. And we start to see quite a few of those now, which gives us heart that actually the policy is working, that the education message is getting out there. But we also recently did a survey of our insureds and asked them *"how many of you have cyber cover?"* And more than half said they didn't. We were like, yes, you do, you've got it with us. You already have it with us. So, I really want to get across the message to people that they already have cyber cover. It's free, it's automatic. You don't have to apply for it. We bought it for your benefit, so don't feel afraid to use it and just understand a little bit about what it covers, because it's a benefit that you get when you insure with us for your professional indemnity.

Julian: And don't feel that the threshold for taking advantage of that benefit is a financial loss.

Elissa: No, no, all that you need to have is a cyber breach. Actually, all you need to have is a suspected cyber breach, so it's actually just suspecting that you've had a cyber breach that allows you to access that policy.

Julian: And if you are in that nervous situation where you think there might have been a breach, how do you best get in touch with Lawcover? Are we talking about a stamp, self-addressed envelope, popped in the post or something like that, or is there an easier way?

Elissa: Carrier pigeon maybe. So, there is a hotline that you can call.

Julian: Well, a hotline sounds like a much more efficient way to get in touch. What is the hotline number, Elissa?

Elissa: So, the hotline number is **1-800-427-322**, which is **1-800-4-BREACH**, and it's staffed 24/7.

Julian: Fantastic. Elissa, thanks very much for joining us on Risk On Air.

Elissa: No problem, it's an absolute pleasure.

Julian: And thanks very much for listening. I'm Julian Morrow. This is Risk On Air. We'll be back with you shortly with more useful tips.

Outro

Lawcover's group cyber insurance is underwritten by Tokio Marine Kiln and is subject to the full terms and conditions of the policy wording. To view the policy wording and additional cyber tools – go to lawcover.com.au and type "cyber risk insurance" into the search bar.

Thanks for listening to Risk On Air by Lawcover. Join us for the next episode on current risks and legal practice to stay up to date.