Episode 45

Cybercrime – How you respond matters

Intro

This is Risk on Air by Lawcover. Today's episode: Cybercrime – How you respond matters.

Julian: Welcome to Risk on Air. I'm Julian Morrow, and I'm joined today by Malcolm Heath, Lawcover's Practice Risk Manager, to discuss a five-letter word that could also be a four-letter word: cyber. It's a huge area of concern for all businesses, but particularly law firms. It's listed in many surveys as the biggest operational challenge that law firms are facing, and it's something firms across the spectrum have to be absolutely focused on. Isn't that right, Malcolm?

Malcolm: That is exactly right, Julian.

Julian: Now, how big a challenge is cyber for law firms at the moment?

Malcolm: Interesting question. On one hand, it's an enormous challenge because of the size, and scale and ongoing nature of this crime. Yet, at the other end of the spectrum, it's actually very manageable to minimise the impacts of cybercrime. So, on the scale of this enormous crime that's really only 10 years old now and really, for the legal profession in Australia, about eight years old in terms of professional negligence claims, so it's a new area of crime. At the top end it's a huge issue but we can manage it fairly effectively with fundamental improvements in what we do.

Julian: And it's interesting that you say minimising the risk. I think there was a time where, perhaps, we thought that, *Oh well, that might happen to someone else, but it's not going to happen to me.* Really, these days, you have to approach things on the basis that it is going to happen to all of us at some point and you've got to get the processes, systems, and the mindset in place for when it does.

Malcolm: Yeah, that's really important - to think of the mindset. I think that's the first part to understand the size and scale of it and also to understand that I have to change and if I've already changed, I have to keep on changing and improving, because we can't get to base count one and think *We've done it, we're finished.* And that actually happened with a firm who had a cyberattack and it was found out that they did their training some years ago and nothing since, and they were left vulnerable as a consequence of lack of follow up. So it may have been a tick box exercise to do that initial training - *We've done that. That's fantastic. We're all aware now and we won't fall for those easy traps* - but they did.

Julian: Isn't that interesting? Because the top types of cybercrime that are reported are pretty familiar - email compromise, particularly business email compromise, and online banking fraud. But the techniques within those categories are changing all the time, and so the training that you got last time might not equip you for what the scammers are up to these days. Very true. The psychological aspects are getting more sophisticated, the techniques are improving, and that's where we have to adjust and remind ourselves never to think *I'm on top of it.*

Julian: And is this something that you're actually seeing at the claims level at Lawcover, Malcolm?

Malcolm: Yes, it's ongoing. We still see the business email compromise issues. We still hear from the principals, *"I never thought they were going to be after me or my firm I'm a small law firm, why would they be after me?"* And they've sort of personalised it, which is a mistake, rather than thinking the criminals are looking for vulnerabilities in systems and that's what they're after, rather than after Julian Morrow or Malcolm Heath.

Julian: And it's interesting from what you're saying there, you're seeing the risks popping up at firms of all sizes.

Malcolm: Oh, absolutely, and particularly smaller firms, who may be more vulnerable in the belief that, *"Oh, they're not after my firm"* or they're operating on a tight budget and are not investing appropriately in IT security and in the education.

Julian: So, let's talk about what you should do if you find yourself in a situation that you know there's been a breach, or you just think there might have been one. How should a practitioner in that very, very unwelcome place respond?

Malcolm: Yeah, and that's very important too, to think we may have. Rather than it being definitive, let's be a little bit proactive and do an investigation where we think there's unusual activity.

Julian: Yeah, so if you're in that really unwelcome position, how should a practitioner or a practice manager or anyone in a law firm respond?

Malcolm: Firstly, they should contact their IT service providers. Depending on the size of the firm, they may have an internal IT team or their external provider, and these are the days now for the smallest of firms to have an IT support service available and contactable. And also, they can notify of a potential problem under the Lawcover group Cyber Risk Insurance Policy. That's the policy that coincides with the Lawcover Professional Indemnity Insurance Policy. So for a firm that's opening up for the first time, they will have their professional indemnity insurance policy but automatically there's a foundational level of cover with the Cyber Risk Insurance Policy. If the firm's renewing the same process, they're renewing their professional indemnity insurance, automatically that Cyber Risk Insurance Policy comes into play. Foundational level of cover, but very important and there's a number there which is so important to note, which is **1800 427 322**.

Julian: **1800 427 322**, or sometimes referred to as **1800 4BREACH**. Now you can call that straight away.

Malcolm: Yeah. The lines are open now. Yes, you can, and that can be very supportive. It can immediately relieve the pressures on the solicitor, knowing that, okay, there's technical expertise at hand - either through their competent IT provider or through the Cyber Risk Policy - to discuss a process going forward.

Julian: So, not only have you formally notified your insurer, you're actually in touch with someone who deals with these issues all the time and can give you the practical advice that you might need, and probably is feeling a little bit more calm than you are when you call.

Malcolm: That's exactly right. Very good point, too, about that pressure when we're anxious.

Julian: Yeah well, you've alluded to the fact that this has been an active area of claims for Lawcover. Could you give us a sense of what sort of situations it's been that have happened within a law firm that have led to a claim being made?

Malcolm: Over the last 12 months, we've seen an elevation in telephone fraud, impersonation fraud, whereby the impersonator is allegedly calling from the law firm's bank and they're speaking to the partner. They've been directed through to the partner, and they are talking about identification of unusual activity in the law firm's trust account.

Julian: Right. So the scam is, it sounds like you're being alerted to unusual activity in the account, but in fact, the call itself is the scam.

Malcolm: That's exactly right. So, the scam is talking about a scam and when we mention trust account, peculiarities, uncertainties to a solicitor.

Julian: Red flags

Malcolm: Red flags and heart rate escalation.

Julian: Making me nervous, just talking about it now, Malcolm.

Malcolm: It's making me get goosebumps about it too. Heart rate may be from a normal resting pulse or working at the desk pulse, leaping up towards 200, 220. With that type of information. Now, the behavioural response when we hear this, it's connected as an extreme disaster for the law firm, we are then thrown into a state of anxiety, and it's at that particular point that the fraudster is able to do their best work because of the panic that's building, and when we're panicked, we don't think straight and we do actions that we would never normally do in a calm state of alertness.

Julian: You can see that, essentially, the fundamental purpose of the scam is to get you into that state as quickly as possible, because most scams are the result of human error, and when we are anxious, maybe even panicking, that's when those errors are most likely to happen.

Malcolm: That's exactly right, and the fear that comes into play its fear driven for the practitioner is significant and they want it to stop.

Julian: It's also a real challenge, isn't it? Because your intuitive response in a situation like this would be *Well, I need to speak to the bank,* or you might feel like you are speaking to the right person while you're being scammed. So how do you deal with that?

Malcolm: Yeah, this is the thing where it seems when we're talking about in the cold light of day, *I would never do that, I wouldn't fall for that. I would always hang up and call the bank myself,* which is exactly what should be done. But when we're in a panic state, it's really fight or flight. And this is to try and stop the problem that's occurring in the law firm's trust account, with clients' funds potentially going elsewhere. And so, this is the point of call - who's helping? They've alerted us to the problem, they're here to help.

Julian: It's interesting because what we're talking about is, if it's actually happening, an emergency. But what you just said there is that good practice is probably to put the phone down and call back. Isn't that introducing an element of delay into an emergency scenario, Mal?

Malcolm: That's right, because it allows you to collect your thoughts and think of the process in a crisis.

Julian: We're not saying go on annual leave, take a holiday and look at it in a couple of months.

Malcolm: That's right

Julian: But give yourself a moment and put a break in that, in the cycle of worry.

Malcolm: Exactly, it's a pause. It's important to pause and treat it like okay, this is a crisis. I'm like a first aid responder, so I'm not going to run over to the victim because my running across the road puts me in immense danger and then I cannot help that person that I actually went out to try and help. So I've defeated the entire purpose - it's far better for me to look around and check my own safety. When I understand that it's clear, I can walk across to that victim whilst thinking about the process I'm going to take in triage, whilst comfortably getting out my phone and dialling 000 and thinking about the location, to report where I am as well, and going over to the person who's injured. So there's a whole variety of calm thinking that we can do to better manage a crisis. So it's very hard to transfer that thinking into a calm office environment, but that's the discipline and the changing behaviours that we need to think about when we have those left of field calls.

Julian: And it's also a situation where different people are going to respond in different ways. And to extend the analogy if you go into an emergency department at a hospital, what you see and what those departments rely on is teamwork - more than one person being involved. Does the same apply to cyber risks for lawyers, Malcolm?

Malcolm: Absolutely. It's a great analogy to look at the team and the support that's available. So, that is your IT security. It's another colleague within the firm. If you are a sole practitioner operating by yourself and you don't have a colleague in the firm or your IT team, you can contact another colleague that you've got a trusted relationship in and one that you know is a sound, rational thinking colleague. Make sure you call your bank's fraud team. Or, if you're nearby, if you're a suburban firm, walk to your bank and go to the bank and speak to them there. Minutes will not be the difference between total disaster and far better management.

Julian: Yeah, yeah, and often it's about making sure that there's an independent line of communication initiated by the practice themselves, not something that's coming in externally, because that's where the scams come from.

Malcolm: Exactly, we need to be street smart and aware - not totally suspicious of everybody and everything, but that awareness when there is something left to field.

Julian: And putting in place steps in the process - simple opportunities to take that breath, to pause and to restart communications in a way that you can internally say, *Yeah, I know that this is actually going to be a safe communication*. How do you think law firms are going, Malcolm, in terms of prepping themselves for these sorts of scenarios and then dealing with the possible or actual cyber crisis when it comes?

Malcolm: There is a gigantic spectrum of well. Some are doing it excellently, they're at the best practice level, and others are still back 10, 15 years in their IT security and in their thinking about their systems and processes in their firm, and that's driven by a number of factors that can come into play. It's a lack of awareness or understanding, financial pressures, we can't invest in appropriate IT security and support services, we are in denial stage and there's a whole spectrum in between.

Julian: And what about basic stuff, like password security and multi-factor authentication? Are firms, big and small, doing well on that front?

Malcolm: Mixed. Like everything – mixed. It is imperative to have password protection, complex passwords, and they're changed on a regular basis across all endpoints of the law firm's computer systems. Not forgetting our handheld devices. If we are operating work from our handheld devices, the security level on those should be as robust as the law firm's computer system as well. Virtual Private Networks are important. Free Wi-Fi, public Wi-Fi should be dismissed, and password protection, Wi-Fi multi-factor authentication is very important as well on all outputs, and that's what we're still seeing when there's been a business email compromise, that many firms still haven't implemented multi-factor authentication across all their law firm's computer systems endpoints. So, it allows simple entry - once the criminal has accessed the firm, we know with business email compromise they'll go into Microsoft Outlook rules, they'll change the rules, redirecting emails as read and into an archive box or a delete box or another sub-inbox that the solicitor or support staff member never really looks at. Then, they've got all the time that they need to read and manipulate information within that email change addresses. They can put in rules to redirect the client's email to their email that they want to use, and in recent examples that has happened where the criminal is liaising directly with the client of the law firm, the client thinks they're liaising with the law firm, but those emails are no longer even reaching the law firm in the archive box. They've been redirected by the Microsoft Office rules that have been manipulated by the criminal. Sometimes phoning the client periodically throughout a transaction, knowing that it's the client's phone number that you've got from the original file, not from the one in the email, to confirm information, to give them an update.

In the scenario I've just been talking about, they may say *But I've sent you all that information and you've responded,* and there's the red flag straight away saying well, actually, *No I haven't, I haven't received anything, and I haven't responded.* And you know then that there's a potential problem and then can make the appropriate investigations, rather than if we are solely relying on email communications as our only source of communication with the client. That's now a much higher risk than it used to be.

Julian: And a timely reminder there, Malcolm, that looking out for the best interests of a client involves not just thinking about your own systems and people, but also your clients' systems and people, because a breach on either end could be disastrous.

Malcolm: That's right. So, we're seeing many firms improving their own security systems, their education and training and implementing all the appropriate things, and that's fabulous; however, are they having the conversation with their clients about cyber risk? Simply, you know some simple mechanisms - like if I've been directed to transfer $700,000 into a law firm's trust account, why don't we do a test of $10 before I potentially send $700,000 to a criminal's account? It's that type of thinking that we need to change, simple things, to look at better protections. One small firm saw a practitioner right on top of it saying *"Yes, you know what I do? I always meet my clients face-to-face",* so there's the perfect client identifications and would provide the client with a code word. That can be a simple way so, when they call, when it's to do with critical information transfers, such as funds transfers.

Julian: And it's interesting, it seems like a way that you can be improving both your cyber security but also the relationship with the client. You're making it more human and personal in a way which is good for the broader relationship, while you're minimising your cyber risk.

Malcolm: That's so correct. Yes, it does take time, but there's an investment in that time that it takes and it's providing a higher security level for your clients and giving greater confidence to your clients.

Julian: We've been focusing on, if you like, the psychology and mental preparedness required for these sorts of situations, Malcolm, but it's worth probably also mentioning the changing regulatory environment as well. There's an increasing intertwining of cybersecurity issues and privacy issues and regulation as well. Any comments on that?

Malcolm: Yeah, there's a raft of legislation coming through changes in the Privacy Act. There's still the $3M threshold, which alleviates some of the responsibilities for smaller organisations to have to report on notifiable data breaches. However, that's likely to change. The great, great majority of our firms who we insure have turnovers of less than $3M and they will need to be on the front foot about responsibilities in notifying.

Julian: Yeah, so recent changes to the Privacy Act, the cyber security legislation went through, but this is a very active area. Prospect that there will be more changes along the lines. That's something that you've really got to be making sure that you're up to date within your knowledge.

Malcolm: Yes, and I think the important point which you touched on earlier was it's a collective. We can't try and deal with this individually. The criminals work in clusters and groups and communities. They're sophisticated and clever and if we try and defend this alone, we will be targeted. And keep on learning and look at it in a positive light - there are always opportunities. We can get a competitive advantage - if I'm working on my firm's security and confidential information and I'm looking at encrypted services and I'm able to communicate the level of competencies to my clients to give them a higher level of confidence themselves, that may put me in a far better position going forward.

Julian: Well, Malcolm, it's been fascinating discussing the latest cyber risks and how to respond to them. Something tells me the conversation will need to continue, so let's have another chat another time.

Malcolm: Thanks, Julian, thanks very much.

Julian: And of course, there are plenty of cyber resources on the Lawcover website. Go to lawcover.com.au. Or, if you do need to get in touch by phone any time of the day or night because you've experienced a possible breach, that number again is **1800 4BREACH** or **1800 427 322**.

Outro

Thanks for listening to Risk on Air by Lawcover. Stay up to date and join us for the next episode on current risks in legal practice.

Resources:

lawcover.com.au