Risk ON AIR

Cyber Series

Transcript

Lawcover's Cyber Risk Insurance Policy

Intro

In part 4 of Lawcover's cyber podcast series, host Julian Morrow talks to Katherine Jones, partner at Colin Biggers & Paisley, about Lawcover's Cyber Risk Insurance Policy that Lawcover has put in place for the benefit of its insured law practices.

Julian: Welcome to Risk on Air. I'm Julian Morrow and today we are joined by Katherine Jones, partner at Colin Biggers & Paisley Lawyers, the firm that handles claims on Lawcover's Group Cyber Policy.

Welcome, Katherine.

Katherine: Hello.

Julian: Is the cyber risk that law practices face these days just part of the general risk that all businesses and people have to confront, or do you think that law firms are a particular target of cyber criminals?

Katherine: Probably a bit of both. In Australia, there is a cybercrime every six minutes, so it is definitely not something restricted to law firms; it's Australia wide. But law firms in particular are a target. We have seen an increase in the number of notifications for law firms and really, I think the key reason can boil down to a couple of things. The first is who our clients are. If you're a big firm, you could have a lot of government or defence work, and that's really important precious information. And then you could have family law or estates, and that too, has a lot of personal and sensitive information about individuals. Law firms also handle high volume of money. I mean conveyancing in Sydney - you'd be hard pressed to buy a house for less than a million dollars in Sydney – so that money has to go through lawyers at some point. So those factors really mean that lawyers are targeted.

Julian: And when we think about a law firm setup, are there particular places within a law firm or areas that you would describe as high risk?

Katherine: Yes, I have seen so many admin accounts targeted. It's often the forgotten account. It's the general email address for reception or support and it's just not monitored like other accounts. People who handle accounts as in money are very targeted in a law firm.

Transcript

Lawcover's Cyber Risk Insurance Policy

Julian: And what about in terms of the tech setup of a firm? You mentioned the email addresses that are the generic ones that maybe don't get as much attention. Does the same apply in terms of the hardware setup?

Katherine: Yeah, the hardware for law firms is interesting. Just generally, I don't think we've managed to keep pace with the way things develop. I mean, we're lawyers, we do law, we're not IT people. We really have this collective idea that that's someone else's problem. We outsource that, but we as lawyers need to be across it and know what's happening in our systems, because they are vulnerable.

Julian: Are there any other things on the sort of hardware and tech side that you regard as particularly high risk?

Katherine: I think legacy servers.

Julian: So, what's a legacy server?

Katherine: So, if you've got a practice that's merged or acquired another practice and most of their information gets transferred over but there's those annoying files that can't be supported on the new network, or not everything's completely transferred over, and you maintain this other server, it is a massive risk because it's usually in the back room, not updated.

Julian: It's not getting the attention, not front of mind, but still carrying information of equal value but greater vulnerability.

Katherine: Exactly, and often they are internet facing, so they're a point of access for a threat actor.

Julian: And what about things like even just more human practices, like sharing devices and things like that? Is that a problem?

Katherine: Yeah, so I'll answer this with a story. Two weeks ago, I received a notification and, as we dug into it, the notification was that all of the emails for the practice admin account kept being deleted and it seemed like it was a software glitch. We couldn't actually forensically work out what was happening. And when we took a step back to try to unwind, how could this happen? - there were six users within the law firm who were sharing logins, who had the same account on each of their personal devices as well as their laptops, and were sharing that access through a shared VPN. So, so much of that information, forensically with an audit log, gets combined that we couldn't work out who was accidentally sitting, maybe at home at night, swiping on their phone, tidying up the inbox and not realising that they were impacting the emails that everyone was looking at because they were sharing it, and that's a common issue that we're seeing.

Julian: That's really interesting as well, because that's, I suppose, an example of where little workarounds or efficiencies that might seem very appealing can actually be the latent flaw that can cause a critical incident.

Katherine: Yeah, and I can completely understand. You know they were trying to streamline the process. How do we share the information better? We can all just have access to this one account. But it was backfiring.

Transcript

Lawcover's Cyber Risk Insurance Policy

Julian: As you mentioned, you get the notifications on the Lawcover Group Cyber Policy. What are the most common ways that cyber criminals gain access to law firm email accounts, which you've already mentioned a couple of times?

Katherine: Yeah. So, a handful of ways would be the most dominant. The first would be stolen credentials. So, the details of the individual have been compromised somewhere. I mean, I don't know how many of us have received Medibank and Optus notifications. If our personal information has been caught up in that - our logins, our passwords - then it blows on if we haven't changed those passwords. The same can be true for your work email. If you're putting it down as a login, it too can get compromised.

The other way would be phishing. Phishing's really quite sophisticated now. Phishing really only works if you're expecting the email from someone. So, if it's your personal account, and you get an email from Pet Barn but you have no pets, it's not going to work. You're not going to click on it, you're going to delete it. But if its your work account and you get an email from Dropbox saying this client has uploaded material and you're actually waiting for that material, you're likely to click on the link without verifying that it's actually authentic. So that has really been an increasing area that we're seeing. The other way is just malware, you know, they've broken into the system.

Julian: And I suppose phishing is a good example where it's a category that probably we've been aware of for a long time. But even within that, the methods can change over time as the technology changes, but also as the cyber criminals get more sophisticated.

Katherine: Yeah, AI has really changed the whole way phishing works because they can customise, on bulk, notifications that go out to people, and if their hit rate's 1 in 1,000, that's still a pretty good hit rate.

Julian: So you really see, at the coalface of notifications, you see changes in the methods that lead to claims or inquiries?

Katherine: Yeah, definitely, the changes with the phishing have been quite obvious. The other way that we've seen quite a lot of notifications is it's almost not even the system being compromised, but PDFs along the way are being intercepted and compromised, because people have this belief that PDFs are secure; they're locked. But they're not. Everything can be changed, and that's something that's definitely on the increase.

Julian: That is also interesting, in a slightly terrifying way.

Katherine: Yeah, it's all terrifying.

Julian: Exactly. So, when you mentioned the PDFs, is it a combination there of things like links embedded in PDFs, but also just information changed in a document which, because of the little dot PDF, you think oh well, that must be fixed.

Katherine: Yeah, people just have this safety that comes with a PDF. Let me be the first one to provide this message. It's not really true. Where they've managed to edit the PDF and change the bank account is the most common, and that step of verifying the bank account has not happened because there's this belief that, oh well, it's a verified PDF, we're good to go.

Transcript

Lawcover's Cyber Risk Insurance Policy

Julian: Well, as we all just reel from that information about PDFs, let's go back to the emails. Is it possible to say what a cybercriminal will ordinarily do or the types of things that they will do if they do get access to a legal practitioner's email?

Katherine: Yes. So on average, I would say that business email compromises are one of the most common notifications that we see. And that means usually that the email account of the practice principal or the admin account or the solicitor's account has been compromised and is used to facilitate the fraud. Usually what happens is the criminal has gone into the account, sometimes sits and watches the account for a little while and they work out, okay, I'm expecting john@abc.com to send me an email asking for the final details so we can transfer the money. They will see that, and they will intercept that email, change the details, but also set up an inbox rule in your account so that when John replies going got the confirmation of your email, you don't see that. It goes automatically to another file, usually the RSS file. So, it looks like the email is coming and going from your email account, but you're completely unaware.

Julian: And again there, the interesting point that familiarity from an email chain, while it might seem like a point of assurance, can actually be the critical point of vulnerability.

Katherine: Yes, and we are very trusting. As lawyers, we really think that, oh well, I trust them. That must be correct. Unfortunately, it's not a question of trusting each other. It's criminals who have intercepted the process that we need to make sure are not going to interfere with someone else's money.

Julian: So, let's talk about what happens when the Lawcover Cyber Group Policy is relied on. How does that policy apply in the event of a cyber breach?

Katherine: So, the Lawcover Cyber Risk Policy is a group policy. It is taken out by Lawcover on behalf of all of its insureds, so everyone has the benefit of the emergency response provided under this policy that Lawcover has got for them, if you have PI insurance with Lawcover. The policy is intended to really help you through those first few days of what is a very stressful situation and working out what has happened, and to put you back into the position that you were prior to the breach.

Julian: So, it's all about the emergency response in that first phase.

Katherine: It's the first phase. It is, what technical support do you need? What privacy advice might you need? Is your IT service provider working overtime, five days in a row, all night long, trying to get your systems back up? Their costs could be quite substantial, so looking to cover those costs. If you're involved in a ransom, there is cyber extortion cover. So potentially subject to a whole bunch of things, including anti-money laundering, there could be cover. The other angle is also business interruptions. So, if you are subjected to a ransom, there is a waiting period, for I think it's eight hours under the policy, but then if your business is severely impacted, there might be cover for some of those business losses.

Julian: And it's because Lawcover is actually the insured in this case, as opposed to in their professional indemnity policies, that people come to your firm on notification. How do they get in touch if there's an incident?

Transcript

Lawcover's Cyber Risk Insurance Policy

Katherine: So, there are two ways. We have a 24/7 phone number that you can ring, which is 1800 4BREACH, which comes out to be **1800 427 322**. We also have an email address, which is lawcyber@cbp.com.au, that you can email and someone will be in contact with you very quickly.

Julian: When you get a notification, what are the first things that you do or that you advise firms to do if there's a suspected breach?

Katherine: So maybe we should do this as a story because it's often easiest to think of it in an example. Let's say, Julian, you're working on a conveyance. Lucky you, you have a beautiful house in Sydney that has sold for $2.5 million. Settlement is tomorrow and you've been arranging all of the details. It's largely going to go through PEXA, but you've got bits and pieces that you've been emailing your client about and hopefully the settlement will progress tomorrow. You have received a call from the client this morning asking why you were chasing again for some more money. It doesn't quite make sense because they sent that money a week ago. I'm confused why there's more requests for money and you pause and you think I actually haven't sent you a request for money yet. I've been waiting for the final payout figures from the other side.

Julian: Start raising those red flags.

Katherine: The pit in your stomach immediately forms. You check your email account, no, you can't see anything sent. What is going on? And they send you a confirmation of payment. All of a sudden you think, well, there's a fundamental problem. Either I'm compromised or they're compromised. What do I do?

You call us and then we will take the story because we need to know how much has been involved, where the breach might have happened. How long are we talking? Has it been months? Has it been days, hours, since that money was transferred? What do we think has happened? Once we've triaged the situation to work out whether it's urgent or not, for example, an active ransom would be an urgent situation. If it's not so urgent, still high priority we would look to appoint IT forensics. If your IT might not be able to do any forensics or they're too busy trying to deal with the current situation and we have panel providers who we frequently use who can run IT forensics for us quickly, we could look and see if you need some comms assistance and then later on we'd look at the other things like privacy and individual notifications and cover under the policy, but the immediate response is really almost always IT based.

Julian: And you use that expression IT forensics. What do IT forensic investigators do when they're appointed?

Katherine: They usually deploy remotely into your system, which can cause some people quite concern.

Julian: I can imagine. *Another* remote access?

Katherine: I was like sorry, what? No, so they'll deploy remotely into your system with your permission and deploy endpoint software onto each device and terminal and run diagnostics on it to see have there been any strange logins? Has there been a massive spike in the amount of data that's been taken from that terminal in the last 24 hours?

They're looking for that type of information which can immediately tell you where the compromise might be, whether that's on your system or the client's.

Julian: And how long does that sort of take?

Katherine: We can know within hours whether it's our client's system or whether it's the other side. It's quite fast.

Julian: Well, that's reassuring to hear, and I suppose it means that lawyers can probably, in most cases, be going on with their business while the IT professionals are sort of assessing the system to see what's actually happening under the hood.

Katherine: Yeah, once the triage has occurred and once the IT forensics are in there, it is sort of happening in the background for a while.

Julian: So obviously there are going to have to be IT professionals involved, but, as you've already said, cyber security awareness and knowledge is something these days that legal practitioners really need to have as part of their general business skill set. So what technical tools would you say are the most effective for practitioners in terms of increasing their own cyber awareness and cyber resilience?

Katherine: The first and the most paramount would be having multi-factor authentication on your devices. It just prevents so much fraud. It's a simple thing that you can do. It's actually usually just a button that you tick within your software and it can stop a lot of compromises.

Julian: So, at least for the moment, we're at the stage where multi-factor authentication is a genuine protection. You're not seeing incidents of that getting hacked?

Katherine: Yes, you do.

Julian: Oh, dear.

Katherine: I know, I know, don't go there, don't go there.

Julian: It's almost like there's no perfect security system.

Katherine: There is no perfect or one answer. It is a combination of a lot of things.

Julian: Yeah, but having the multi-factor authentication really does decrease the chance of a compromise.

Katherine: It would. It definitely would. And there's other things that you can do too. You could have your whole system what's called pen tested, so that's having external forensics come in and see, *actually, we can break into your system very quickly.* That's an open door for someone to walk right in and you can see then, *oh well, we better fix that.* Have good security on data, have good backup processes. If you're having a ransom event and your most recent backup is six months old, that's going to weigh very heavily on your ability to make a decision whether to pay or not to pay. The backup is crucial and to have it separated from your everyday system is very important. Have separate users, which we covered off before, and change your passwords regularly. If you have a cycle and your staff are used to having to change their passwords every 20 days or whatever it might be, that's just a good system because it will kick someone out of your network once you change all the passwords.

Transcript

Lawcover's Cyber Risk Insurance Policy

Julian: Yeah, so you're not just refreshing your passwords when you get that notification. Saying that there's been an external breach, and everyone's got to change. Makes a lot of sense. So there's technical factors that individuals can take into account. Are there other things that you would say practitioners should be aware of, or things that they can do to increase cyber awareness and cyber resilience?

Katherine: Yeah, cyber security is a collective approach. It is not the responsibility of IT, it is not the responsibility of the principal of the practice alone. It is the responsibility of everyone and if everyone buys into that, then you've got a great start to having good security. Because then if everyone's trained and fully aware and has the standard protocol of always calling, then everyone is on the same page and the risk minimises fundamentally. That's your internal staff, but also your clients have to be part of the process too. So when you're onboarding them, make sure they're aware, you know, we are targets, lawyers are targets, so we will always call you and request confirmation before we arrange for transfers. Could you please make sure that you take those calls and don't just reply by email? It's really important to our process that we have this conversation repeatedly throughout the life of this file together.

Julian: You mentioned earlier, Katherine, that AI has changed things. Are you actually seeing that flow down in notifications that AI is being deployed and leading to different types of claims?

Katherine: It's hard to pinpoint whether that's actually what's behind some of the notifications, but the consistency of some of the notifications, like I mentioned Dropbox as a phishing link, it has to be. Because the way it's targeted could only have come from an AI sourced threat.

Julian: Well, it's been a great pleasure speaking with you and I think, on the statistics that you gave us earlier, there's probably been about three cybercrimes committed while we've been speaking. But thanks very much for giving us some tips on how to avoid or minimise the risks of being the person to whom it happens. I suppose we should do the infomercial thing and recap the number If you do have an incident, it's 1800 4BREACH, or **1800 427 322**.

Katherine: It is indeed.

Julian: And you can also use the email address lawcyber@cbp.com.au. Thanks very much for speaking with us on Risk on Air, Katherine.

Katherine: Thanks for having me.

Julian: And of course, there's more information about cybercrime and what legal practitioners can do to protect themselves from it on the Lawcover website. Just go to lawcover.com.au.

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 www.lawcover.com.au and type "cyber risk insurance".

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