Episode 62

Calling in the Cops: What the NSW Cybercrime Squad Wants Lawyers to Know

Intro

This is Risk on Air by Lawcover, and in this episode we're calling in the cops.

Julian: Welcome to Risk on Air.

Welcome to Risk on Air. I'm Julian Morrow, and today we are talking about what the New South Wales Cybercrime Squad wants lawyers to know. And who better to ask than Detective Superintendent Matt Craft of the Cybercrime Squad of New South Wales Police. Welcome, Matt.

Matt: Good morning, thank you.

Julian: Now Matt, could you tell us a bit about the New South Wales Cybercrime Squad?

Matt: Sure. Look, we were formed in 2018, so as a standalone squad. As the commander, I'm fortunate that I have approximately 60 staff. Not all of them are sworn, so what I mean by that is carry firearms. We've got unsworn technical experts that work there as well, but most of the detectives that are attached to the Cybercrime Squad in their former life were in IT, or have some sort of tertiary qualification in IT, that they're able to blend their love for all things electronics and policing.

So that works out really well for us as an organisation because they're pretty talented and pretty good at what they do.

Julian: And I understand a lot of the work that you do. There's a wide range of cybercrime, obviously, and the breadth of crime is increasing. But a lot of it has to do with damage to business and business compromise in particular, is that right?

Matt: Yeah, true. So at the Cybercrime Squad, we look at the cyber enabled crime, which is just the use of IT to commit general crime. But we also have a specialist team which look at your ransomware, your malware, data breaches, things like that.

We also police the internet, believe it or not. We have an Online Covert Engagement Team. Now their job... Just because you want to play on the dark web and you want to commit crimes on the dark web doesn't mean that you're immune from investigation and we're pretty good at that as well. So, we've got a range of technical expertise within the squad.

Julian: And in terms of lawyers practising, how often do you come across lawyers as victims of cybercrime?

Matt: Well, interestingly enough, we get to become aware that law firms have been in some way compromised through a number of means.

But what I would say is that we don't have enough law firms putting their hand up and asking for help when they have been a victim themselves. There is a trend that we see, not all the time, where those incidents are tried to be dealt with in-house and not involve the police.

There may be a number of reasons for that and some of it may well be that they don't understand that the New South Wales Police has a very sophisticated, well-resourced cybercrime squad that is able to help because they are a victim, they deserve help and cybercrime is here to help them.

Julian: If you think about that subset of lawyers falling victim to cybercrime, would you say that it's a case of very sophisticated technical attacks that are hitting law firms, or is it more basic problems that are arising?

Matt: Look, a combination of both. Law firms are attractive. I think the evidence would say that sophisticated cyber actors are targeting law firms. And the reason for that is that some of the things that cyber actors really like is money, confidential information - law firms generally have both. So, it's a one-stop shop, unfortunately. And that's a burden that law firms need to consider, that they do hold confidential information that threat actors are able to steal and then make money off.

But also, there's things like trust accounts. They are actively targeted because they understand and these threat actors' research. The bigger firms will generally have a whole IT department that is able to secure their systems. Some of the smaller firms don't have that luxury, so they may be more vulnerable, but it does change in terms of how they're targeted.

Julian: Does the area of practice that you work in make a particular difference in terms of your risk profile for cybercrime?

Matt: I don't think so. If you're a law firm, they will test your systems because don't forget, law firms generally have very complex IT systems. That's a lot to secure. And then when you factor in employees working from home, using their own devices perhaps to access corporate systems, it just adds layers of complexity. And if you're a smaller law firm, cybersecurity may not be front of mind.

Julian: Are most of the criminals, the cyber criminals that you're trying to track down offshore, Matt?

Matt: If we look at attacks on large systems, whether that's government or private, the majority are offshore. But what we have seen, which is very unique to New South Wales at the moment, is over the last three or four years, a significant increase in the number of trusted insiders that are attacking systems. Now, what I mean by a trusted insider, this is somebody that you trust, an employee that's working for you that has privileged access, that then abuse that. So you have a combination of both. So where they are overseas does not mean they're out of reach of law enforcement because we have a range of means to work with our partners, which is important that law firms understand that because if you have an issue, we can help.

Julian: Yeah, because obviously the trusted insider is a particular risk, although I imagine from an investigative perspective, well, it's all inside the jurisdiction and so there might be more that you can achieve there. Perhaps one of the things that is preventing reporting is a perception that the chances of actually getting a result aren't that great. What are the chances if you're a victim of cybercrime of actually recovering something?

Matt: Well, I think it's important to dispel that myth. And that possibly comes down to the fact that it's not well understood how resourced we are and the skills that we have at the cybercrime squad. But if you look at business email compromises, if we just carve that out, which is where the victim is tricked into transferring money by various means.

Julian: The email address has changed a little bit or the fake invoice.

Matt: Yeah, exactly right. So they're losing hundreds of thousands of dollars and that's where they will target trust accounts. We address that problem nationally through the Joint Policing Cybercrime Coordination Centre, which is all of the states and territories, the AFP, the FBI, US Secret Service, we're all in there together, including the banks. So it's a public-private partnership. There's almost half a billion dollars that we've been able to recover where it's reported early. The key is to get on the front foot and report it to law enforcement because if money has been electronically transferred, the sooner you report, the better chance we have of recovering those funds.

Julian: Can you just talk us through a little bit more why it is that the early reporting translates so well to a better outcome?

Matt: So generally speaking, now banks have very sophisticated systems that monitor accounts. If you're not somebody who transfers money overseas, because the fact is that the money will generally end up overseas, and they try and transfer it directly out of your account directly to overseas, that will be flagged as suspicious. The banks will put a hold on it, as they should. So, they will often move it around different mule accounts within Australia before moving it overseas. So, we're able to take advantage of that and working with the banks because they work with us, sitting at tables right beside us - and the primary point is to stop the money. So the sooner it's reported, the sooner we can work with the banks. They put a freeze on it until we can sort out what's occurred.

Julian: That's really interesting, the fact that as a way of evading the automatic triggers that might happen with international funds, it means that there can be money bouncing around in Australia. Yeah, I can see how that could make a big difference.

Matt: And we've even had, working with the banks, where we've monitoring mule accounts and we see, for instance, say $200,000 drop into that account. There's been no crime reported yet, but we just know that that's a suspicious transaction. So we can then start and work back and go and knock on the door of the victim and say, "Hey, have you lost $200,000?" And then they would look and go, "Well, yes, and I didn't really authorise that or I don't understand why that transaction has been made." And we're able to recover that. So it works both ways. We're proactively looking at mule accounts, but also reporting early means that we can respond quickly.

Julian: When you think across cybercrime matters that have involved lawyers and law firms, what would you say beyond quick reporting are the most common things that could prevent the loss that's occurred?

Matt: So I think it's about education of staff. So you need to have established systems where if you're going to authorise a transaction, it needs to occur in this way. That's written down. Staff understand that. So therefore, if, for instance, they get a phone call from a partner that says, "Look, can you transfer X number of dollars", with the inclusion of AI, it may be difficult to assess whether that's actually correct. But if there's established processes that said, "I will never make a phone call", or it needs to have this many signatures, or it's followed up in writing, whatever the case may be, there just needs to be those established practices that staff can follow.

Julian: And in terms of reporting, what's the process you'd recommend for if a law firm is a victim, or I suppose if their client's a victim. There is a range of different agencies, as you've talked about, that are involved in this space. Is there a one-stop shop for reporting?

Matt: For cyber related matters, you have ReportCyber. which is a Commonwealth Government system whereby people can report online 24-7 and then that goes to the particular jurisdiction that victim is domiciled in. You can attend your local police station, but the quickest way is probably ReportCyber or attend your local police station. We have teams on call 24-7, so if it's too big for your local police station, they will contact us.

Julian: A lot of law firms understandably worried about reputational risk associated with not just the fact of cybercrime, but I suppose people being aware that they have had a cybercrime occur. Is reporting confidential?

Matt: Whether it's a law firm or another private business, we're very conscious of that. Now, the media doesn't assist our investigation, so it is confidential. But as lawyers will know, if we end up charging somebody, as soon as we put somebody before the courts, information is released. But that just needs to be managed. Law firms need to remember, they're a victim of crime. They deserve the support of the police and they'll have it. And we can be confidential.

Julian: You mentioned earlier ransomware. Is that an increasing category of crime and what should lawyers do if they find themselves in that invidious situation?

Matt: Exactly right. And if out of today's session, if law firms go back and actually look at ransomware and their response to ransomware, I'd be delighted. It is a big issue for law firms. So generally what we see now is that they will attack the system, get in, copy your data and then encrypt your files, and then they will essentially hold you out to ransom wanting cryptocurrency for the unencryption of your files.

Each firm needs to have a ransomware response plan. What are you going to do when this occurs in terms of communicating with your staff, managing the incident? How are you going to report it? Having most of your decisions made prior so that in the heat of battle when things are occurring, and it will be complicated, you're not making decisions off the cuff. And that includes, are you going to pay ransom? Because if you are going to pay a ransom, how are you going to actually pay it? It's not like you can just meet somebody on the corner in exchange for a bag of cash. It's complicated, but you need to have an incident response company. You need to have a trusted set of people that can come in and assist you to manage this process. And that includes reporting to law enforcement because there are lots of things that law enforcement can do to assist you manage that.

Julian: So you need to have a plan, but as you say, you've got to be aware of the fact that the scene changes, things evolve. Once you've got the plan, what else do you need to do to make sure that you're job ready for the situation that obviously we all hope never happens, but it can?

Matt: And the reality of it will. Like let's be honest, you can't just sit there and think that you're going to be immune from these things. My advice is that plan needs to be reviewed each year and it needs to be desk topped so that your staff understand you have a plan, that it's been reviewed, that as the tech changes with your security systems, that the plan is then updated. Really have those very robust conversations and say, "Well, is this working for us?" Because if you come in Monday morning and all your systems are encrypted, including email, how are you going to achieve that? What are your backups? How long is it going to take you to restore functionality within your systems? Those are the types of things that you need to have.

Julian: And you've seen this happen to law firms?

Matt: Absolutely. It happens to all businesses, government and private. And those companies who have a plan, who have tested that plan, and follow that plan in a time of crisis generally perform better. Like ransomware will always hurt. There's no doubt about that and it's serious criminal offending. But if you've got a plan and you've thought about it, your journey to recovery is often a little bit smoother.

Julian: Let's talk about some of the perceptions that lawyers might have about cybercrime. And you're the expert, you can tell us how true they are. What about if someone thinks, "Oh, we've got an IT provider, they handle that." Does that pass muster in terms of minimising cybercrime risk?

Matt: Look, it's a great first step. As a firm, what you don't want to have is your cousin who likes computers doing your IT. You want to have a professional, which reflects the nature of your business and the confidential information you hold. So it's a great first step, but you want to make sure that they're doing all the necessary steps to protect your system from attack. But also too, what happens if something does happen? What ability do they have to get you back online, particularly in relation to your backups and things like that?

Julian: What about if you think, "Well, look, everyone has multi-factor authentication on all the devices. We should be fine."

Matt: And once again, great first step. Multi-factor, completely agree with it. Encryption is also important, but you need to assess risk. The use of allowing people to bring their own devices and have them interact with your network adds risk to your overall environment. So you need to consider that because whilst they may be using their personal devices to access your systems, they may have other apps and programs on that particular electronic device that can compromise, or provide an avenue for compromise for your systems.

Julian: Matt, how often does it happen that a business, law firm or otherwise, is a victim of cybercrime and they don't know it?

Matt: It's common. We monitor a number of dark web platforms where information is posted and sometimes they're just boasting about what they've done. And we will see that and we will then go and approach that particular victim and alert them to it. And they're not aware. That's pretty common, but we try and be proactive there because at that point we can say, "Hey, this is who we are. This is how we can help. Are you aware of this? What can we do to help?" So it's that good first step for us. That is reasonably common depending on the size of the business. As I said, if you've got a big business where you've got a dedicated IT team that's working, they should have monitoring tools to know when something happens, but sometimes they just don't. When information's posted on the dark web, that will be the first time that we may come across and say, a set of emails, for instance, from a law firm. We found those previously. Well, does that law firm know that they have been compromised?

Julian: How rapidly does the cybercrime scene change, Matt?

Matt: Very quickly. So we may respond a particular way in 2026, but we probably may not be able to do that in 2028. We see changes in the way that offenders interact with victims and particularly with business email compromises. We've seen recently a change whereby it's not just about transferring the cash overseas, they're buying gold bullion within Australia. So that's changed and it comes and goes, or they will move it out in cryptocurrency. So, you do see changes. The actual business email compromise, that's pretty standard, but in terms of the way that they actually deal with the proceeds of crime, that does change. And in terms of whether it's a trusted insider or the particular ransomware variant that's used, that changes all the time as well.

Julian: Is AI changing things in terms of voice simulation and those sorts of things?

Matt: Absolutely. What that means is that offenders are able to scale attacks and replicate them quite quickly. And AI, it's a great tool. And it's like the internet. The internet was a great tool, but it can be used for good and bad. And it's just about that recognition that just because you receive a phone call or a letter or something like that, you need to be a little bit suspicious. It's terrible that in society you need to be that way and think that everybody's out to defraud you, but when you're dealing with confidential information and other people's money, we need to have that "stop and think" approach.

Julian: Lawyers have an obligation to retain documents on their files for a certain number of years. What are the risks that arise with document retention strategies and what would you recommend in terms of how to minimise those risks, Matt?

Matt: Great question, because we all accept that lawyers are in a privileged position and they need to hold on to personal identification information. But at some point, they don't need to retain it any further. Or if they do need to retain it, it needs to be fully encrypted. And we've seen time and time again where offenders have gone in and have taken encrypted files and they do get very frustrated with the fact that it is encrypted. But if every 12 months you go through a process and say, "Right, we now know the law no longer requires us to retain this PII, we should delete it." You shouldn't just keep collecting data forever and a day where you're not required to retain it by virtue of the law.

Julian: Yeah, because there's certainly been cases where personal identification information of former customers from telcos and things like that have stayed on file. And then when the business becomes the subject of a cyber-attack, it's not just current customers, it's also former customers who can be affected.

Matt: Absolutely. And we've seen that in some rather large companies that have been targeted. I think there was one, from memory, it was eight years. They haven't been a customer for eight years. Why was that being retained? And if there is a requirement to retain it, it should be encrypted. And I assume lawyers will have, because of the nature of their transactions, be required to identify individuals.

But then do they need to retain copies of all of that? And if they don't, well, all well and good. I'd suggest they don't. But where they do, that information needs to be encrypted so that if something does happen, it's protected.

Julian: Matt, could you give us a couple of examples of success stories where, whether it's because of early interventions or new techniques, you've been able to actually get a really good result for somebody who's reported?

Matt: In terms of business email compromises, there was a small firm in Western Sydney and they had transferred $250,000 to a bank account, which they were expecting because they were buying goods. So when this invoice arrived, they paid it. But unfortunately, the invoice had been doctored and they'd paid it into the wrong bank account. Now, to their credit, they immediately reported it online to ReportCyber. That flows automatically, so by the time you hit enter on ReportCyber, it's hitting the desk of my staff and they can review it. And we were able to then leverage our contacts within the Joint Policing Cybercrime Coordination Centre with the banks, and we were able to stop and get that money back. It goes to show, reporting early, better outcomes in terms of clawing that money back.

Another example would be, I won't name the government agency, but they were very proactive. So they realised that they'd had a data breach, that the employee had been misusing their information. They identified it quickly, they reported it, and then we were able to respond within 24 hours essentially and secure that data. So yes, data had left the security of their systems, but we were able to then respond quickly and get that data back and lock it down.

Julian: There's a real sense that the rates of cybercrime are increasing. Does the sheer level of reporting to you create a problem sometimes in terms of just what you can actually track down?

Matt: Look, we can't arrest our way out of cybercrime, unfortunately. I'd love to, but the number of people we are arresting and charging each year is increasing. But more importantly, and on the flip side, where we spend a lot of time is prevention disruption. And where somebody reports a matter to us, they may not necessarily always get a criminal investigation, but what they will get is a call or some information about how not to become victimised as a consequence of this again. So we try and teach victims how not to become a victim again because prevention and disruption is very important.

Julian: So just finally, one final message for law firms from the Cybercrime Squad. What do lawyers need to know?

Matt: Look, I'd advocate that you need to prepare. At some point it will happen. You need to think about how you're going to respond. Have a list of the contacts that you will respond, which should include police. We will treat your matter confidentially. And law firms, generally speaking, deal with a lot of confidential information. But allowing that to be just freely transmitted over email so that you've got documents, somebody's driver's licence, passport is all just sent via email, it's just really not a secure way to be transferring somebody's personal identification information.

Matt: Because we've seen before where breaches happen and it includes the whole email box of law firms or accountancy firms or government agencies and therefore every document has been exfiltrated out and is available.

Julian: What are some practice management steps that you could recommend for law firms to keep in mind to make sure that the policy is not set and forget?

Matt: My view, whether you're a big or small business, you need to have cybersecurity as an agenda item at your monthly meetings because it changes so quickly. The number of staff you have coming and going, the number of clients you have, it's constantly changing. So by having it as an action item, it is something that you're constantly turning your mind to, which is important.

Julian: Well, I've got to say, as interactions with the New South Wales Cybercrime Squad go, this has been a very pleasant one.

Thank you very much for joining us on Risk on Air.

Matt: Thank you.

Julian: And of course, remember that cyber insurance cover is automatically provided to all Lawcover insured law practices. The policy is designed for rapid response and crisis management. If you suspect that there's been a cyber incident, contact the Cyber Response Team on 1800 427 322. The team provides access to specialist support for responding to cyber incidents, recovering systems, obtaining expert assistance and managing privacy and other regulatory issues. And remember that the Lawcover Cyber Risk Policy is most valuable in the first few hours after any suspected cyber incident, no matter how big or small.

Outro

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

Resources:

ReportCyber

Lawcover Cyber Risk Insurance