Lawcover™

Risk ON AIR

Cyber Series

Transcript

Data and Privacy Breaches

Intro

In part 2 of Lawcover's Cyber podcast series, host Julian Morrow chats with Nitesh Patel, Principal, and Cyber and Technology Specialist at Gilchrist Connell about data breaches and what a law practice can do to protect its confidential information.

Julian: Welcome to Risk On Air. I'm Julian Morrow, and today we're joined by Nitesh Patel, Cyber and Technology Principal at Gilchrist Connell to talk about "It's not if, but when! Data and privacy breaches; are you at risk?"

Executive summary: now and yes. But let's move on. Nitesh, welcome.

Nitesh: Thanks for having me.

Julian: Well, let me put that proposition to you. Do you agree that for law firms, and in terms of data and privacy breaches, it really is not a question of if, but when?

Nitesh: Yeah, it's the same for all businesses really, if you are relying on the internet, which is basically all of us.

Julian: A lot of it is around the internet these days.

Nitesh: Absolutely, we rely on it so heavily. We've adopted it into our practices at a speed where we've really taken on board the benefits. But to some extent, we haven't really thought about how to protect ourselves and we are trying to catch up in many respects. But that's a long-winded way of saying, yeah it really is, now, not will we be a target or will we be compromised and will we suffer a data breach, but when will this happen.

Julian: Because the rates of these things happening, it's up yeah?

Nitesh: Absolutely. There's some question around whether or not it's more a matter of business is now actually disclosing that they have been subject to these incidents, or they have had data breaches, but all the information we're receiving is that the trend is more and more incidents are occurring, more and more data breaches are occurring. The OAIC in their most recent report indicated that there were 890 notifications of data breaches in 2022. There's a bit of an asterisk on that from my perspective, simply because that applies to data breaches that are notified, and that is generally only in respect of a small subset of the businesses in Australia.

Transcript

Data and Privacy Breaches

Julian: That's the tip of the iceberg hitting our titanic businesses.

Nitesh: That's absolutely the case. And something that's probably worth clarifying here is that we're talking about data breaches and privacy breaches generally. A lot of the focus here will be on criminal activity, malicious actors, cyber incident compromise. But there is a significant human element in all of this and a lot of incidents do actually occur as a result of human error, and one of the key takeaways here is that this is not just a technology issue. This is a human issue and there's a real human element piece around all of this that needs to be very carefully managed.

Julian: Yeah, because a lot of the time there can be sophisticated technological ways of creating the opportunity for a human to make a small mistake that can have very big consequences.

Nitesh: Yeah, absolutely. One of the most common issues that arises is someone has interacted with a phishing email, provided credentials to the system and then that has resulted in a much more significant cyber incident. But leaving that to one side, what about mailing information to incorrect addresses? What about emails to incorrect recipients? Now, as a law firm, that can have some really significant consequences.

Julian: It can also have consequences for the US military recently as well!

Nitesh: Absolutely. So that all counts as a data breach, as a privacy risk as well. Also, the inappropriate disposal of sensitive information. So there's been instances that we've had where sensitive information has been disposed of in the garbage bin, not properly dealt with, and so that in itself is a privacy risk. So yes, the focus here is going to be very much about cyber incidents, but it's always worth having regard to that as well.

Julian: And we said that the number of formally notified incidents is up. Nitesh, do you think that law firms are more of a target than other businesses?

Nitesh: In short, I think the answer is yes. A good starting point is thinking about, well why are malicious actors doing this? In almost all instances, it is for financial gain. And so when you look at a law firm, it has all the key ingredients for a malicious actor. We hold sensitive, sensitive information and that goes beyond personal information. That's sensitive corporate information that can be leveraged very easily for financial gain. Leaving that to one side, we are constantly dealing with large financial transactions. We hold trust accounts and our clients do trust us. So that's all the hallmarks that a threat actor needs or a malicious actor needs so that when they compromise a law firm, they know they've got a good shot of having a significant financial gain, which makes us a higher target.

Julian: And, I suppose also, a law firm will have a host of clients and in a way a data breach at a law firm might be a gateway into a whole series of businesses rather than just one.

Nitesh: Well, absolutely, and that, that goes to something called supply chain risk. We are ourselves a gateway to clients and in many instances where the biggest impact is on a law firm out of a cyber incident is where a client has suffered financial loss.

Julian: So, look, everyone's at risk. But I did wonder – is a law firm's level of cyber risk meaningfully different depending on factors like the size of the firm, or the profile of the clientele, or the nature of the work that you do?

Nitesh: I think instead of looking at it from the perspective of, "Is the extent of the cyber risk different?", it probably is more about "How do you address the risk?" So for example, if you are dealing with particularly vulnerable clients and their information is particularly sensitive,

then that needs to be had regard to. Do you allow personal devices? Bring your own device, is that allowed within your practice? If so, that's a heightened area of risk. How much are you relying on supply chain? Are you relying on third-party suppliers? The size of your organisation of course matters; the bigger the organisation, the greater the expectation of having internal resources to handle the IT and cyber risk. So the particular circumstances of a law firm does make a difference, but in terms of the cyber risk itself, I'd like to think that every business should be treating cyber risk at the same starting point. And then when they're assessing how to deal with cyber risk, that's when you bring into consideration all the various factors of your particular business.

Julian: There've been a number of really high profile cyber security breaches in Australia recently. And I suppose this is a useful time to point out that this podcast is not sponsored by Medibank Private or Optus. It's of course from Lawcover, and obviously, there have been instances that have affected law firms as well. But if we step back and think about just those high-profile data breaches, Nitesh, do you think that there are particular lessons or implications that the general listener could draw from those incidents that we've all heard about?

Nitesh: Yes, I'd like to look at it holistically, I think, because if you look at one particular incident, you might get a particular set of circumstances that have a reason that led to that incident. There's been a number of high-profile incidents. You look across all of them, each of them have their individual unique circumstances, so there's no one way that an incident has occurred. For example, one incident looks to be the result of a bring your own device being compromised. Another one was a phishing email where credentials were provided and compromised. There was a ransomware incident of somewhat unknown origin. There was a supply chain risk that led to a large incident. There's been all sorts of background to all of this, but it shows that you need to look at this holistically.

But it also shows that we've had a telecommunications company of a significant size impacted. We've had a health services provider impacted. Unfortunately, we've had a law firm impacted. We've had a financial services company impacted. There's been a whole range of others that we've dealt with as well. The long and the short of it is that if you're using the internet to provide services, if you rely on electronic means to provide services, which is basically all of us, you need to be taking into account what you need to do to protect yourself from cyber risk. It's as simple as that.

Julian: What are some of the really basic technological pieces and measures that any individual, no matter what scale of practice they're in, could and should take to kind of minimise them?

Nitesh: Yes, from that perspective, I think the starting point is going to be that law firms should always seek assistance from experts if they don't have something internally and that will include a cyber security expert. But some of the basic things are making sure you have proper patching practises to make sure you update and patch your various programs and systems regularly. Making sure you have multifactor authentication, making sure you've got proper backups is a big one that really helps with the recovery and really can help when it comes to data theft, and making sure you've got proper backup procedures in place. So, for example, making sure you've got something that's separated from your network so that it's somewhat protected from a significant cyber incident is important. Password security is a big one. Overarching all of this though is that human element. You really need to make sure you have proper processes, procedures in place, and proper training in place for your staff.

You can have the best technology in the world, but if someone gives malicious actors the keys to the front door, there's very little you can do. One example recently is that we've been assisting a number of businesses actually around scenarios where a phishing email has been interacted with, credentials have been provided, and then on top of that multifactor authentication has been bypassed because access has been granted to the system itself.

Malicious actors are always looking for the weakest link. So they're always looking to update their practices. It just shows how important the human element in all of this is. Having the appropriate approach amongst your staff and making sure they're taking a cautious approach to basically all email communications as a starting point, making sure that your staff are taking the appropriate cautious approach to all electronic communications. Making sure they're undertaking the basic measure of requesting confirmation of payment requests, that's a really big one, and also asking your clients to do the same. Making sure you give them the notices around that. Whether or not that is an actual obligation of law firms, it certainly does not hurt and it can certainly assist you if you suffer a cyber incident.

Of course, the other part is being prepared for a cyber incident. So having a cyber incident response plan and business continuity plans is really important. You want to be having those in place and making sure they're properly tested, making sure they're available offline, it must be tested. You must know what to do at least in a general sense so that you're not guessing or second guessing what your response will be when an incident occurs. And finally, always think about cyber insurance, and I know Lawcover provides a base level of cyber insurance amongst what they provide.

Julian: You mentioned that it's the tip of the iceberg in terms of the numbers of notifiable data breaches. But just to clarify, what is a notifiable data breach and what are the obligations that arise when a firm or any business I suppose, does have a data breach?

Nitesh: Yeah, so that's under the Privacy Act and a notifiable data breach is effectively one where there's been a cyber incident that resulted in the unauthorised access, disclosure, or loss of personal information held by an APP entity, and we'll get to that in a second. That unauthorised disclosure, access, or loss has resulted, or is likely to result in serious harm to one or more affected individuals. And remediation steps have not been taken to prevent that serious harm, and those remediation steps need to be pretty comprehensive and you have to have a fair amount of certainty that those remediation steps have removed that harm.

Julian: So you mentioned APP entities. What are they?

Nitesh: So an APP entity, it covers a whole range of businesses, but there is a significant carve out in place at the moment around small businesses. So if you are a small business that has an annual turnover of less than $3 million, you are not considered an APP entity. There are various carve-backs, for lack of better term. So there is a bit of complexity around that is not as simple as if you have less than $3 million of annual turnover, you are not going to be an APP entity, but effectively that carves out, I believe, up to about 90% of Australian businesses from having to comply with the Privacy Act generally. And that is, though, subject to change; that is on the chopping block and, in all likelihood, I suspect that's going to be removed in the not-too-distant future, and that will bring us in line to other more robust regimes internationally, including the GDPR.

Julian: But for those businesses that are APP entities, what have they got to do?

Transcript

Data and Privacy Breaches

Nitesh: Yeah, so if you suspect there's been a cyber incident that might be an eligible data breach, you have an obligation to take all reasonable steps to carry out a reasonable and expeditious assessment of the incident to determine whether or not it has been an EDB, but for short, and that should happen within 30 days of when you first suspect there might have been an eligible data breach.

Julian: So earlier we talked about Notifiable Data Breaches. You just mentioned Eligible Data Breaches. What's the difference?

Nitesh: Yeah, no, that's a good pickup Julian. So the Notifiable Data Breach regime is in respect of eligible data breaches. Eligible data breaches are the data breaches that satisfy those criteria I just went through that then will result in notification obligations to the Office of the Australian Information Commission as well as affected individuals.

Julian: So if you're an APP entity and you've had a cyber incident, what does that mean for you? What have you got to do?

Nitesh: Yeah, so under the Notifiable Data Breach regime, you need to take reasonable steps to carry out a reasonable and expeditious assessment of the incident to determine whether or not it is actually an eligible data breach. And you need to do that within 30 days of when you first suspect you've had an eligible data breach, which would normally be when you first become aware of the cyber incident. If you take longer, sometimes these things do take longer, especially for larger incidents, the key thing here is you make sure that you've taken copious notes, proper records of all the steps you've taken to try and complete your assessment as reasonably and as expeditiously as possible.

Julian: And so you've said that you've got to do the assessment. What's involved in the assessment?

Nitesh: The assessment is an information gathering exercise of sorts and it's determining whether or not there is a likelihood of serious harm. And so there's multiple parts of this; it is a bit of a complex process. It might seem easy at first, but when you start breaking it down, there's a bit to it. The Privacy Act itself sets out a list of relevant matters, but there's a catchall at the end, which is any other relevant matters.

But to go through some of the stuff that they talk about, it's what are the kind or kinds of information that's been involved? The sensitivity of that information? The protections around that information? Who has accessed it? What is the types of harm that might be involved? And that goes well beyond just financial harm. Tt can be psychological, emotional and other types of harm that you need to factor in and that can be a significant consideration, for example, for the disclosure of health information, or other kinds of sensitive information. The motivation of the perpetrators is always relevant as well. But again, any other relevant matters, and there can be all sorts of things that you need to factor in to determine whether or not there is a likelihood of serious harm to the affected individuals including, before you even get to that point, what is the impacted dataset? That can be trickier to identify than you might first think.

Julian: And as you said, once you've done that assessment, if you think that there's an eligible data breach, then you've got an obligation as an APP entity to notify.

Nitesh: That's correct. And you've got to do that as soon as practicable to the OAIC and any affected individuals. And there's a prescribed format by which you are meant to notify, or at least there's key pieces that you need to include in those notifications. And the critical piece is what steps an individual should take to protect themselves.

Transcript

Data and Privacy Breaches

Julian: You mentioned that some of the thresholds for being APP entities might change. That's because of the Privacy Act review. Is that right?

Nitesh: Yeah, this has been something that's been on the cards for a long time now. The most recent piece in all of this is the Attorney General's released a Privacy Act Review Report in February 2023, and that was a very extensive report that's been subject to a fair bit of consultation. So it's not the be-all and end-all by any stretch, but it gives you a really good indication of where things are going and where we might be heading with all of the privacy reforms. And it's certainly not going to be relaxed, let's put it that way. It's going to be enhanced. One of the key pieces that I mentioned earlier is that there is currently in place a small business exemption; that is very much on the chopping block. It will not be a straightforward removal. So there's going to be a bit of a lead-in. But, effectively that means that if to date you've been relying on the small business exemption, probably a good idea to start thinking about, well, what do I need to do to protect myself? Because leaving aside the Privacy Act, there are other heads of obligations that you need to be thinking about, including what your clients are looking to impose upon you more generally, and what your duty of care might be around cyber risk.

But leaving that to one side, there are a whole range of other proposals that have been canvassed, including adjusting the reporting requirements around an eligible data breach, putting greater certainty around the timeframe, so there's discussion of requiring notification within 72 hours.

Julian: Alright, so certainly it doesn't mean longer.

Nitesh: Certainly not longer. There's also enhanced regulator powers on the cards, a direct right of action for individuals. So in Australia, there's no tort of Privacy, so at the moment, the general course of action for individuals who've had an interference with privacy is to make a complaint to the OAIC, to the regulator. There is significant discussion around including a direct right of action.

More guidance, which is I think going to be very helpful around the obligations that are already in place under the Privacy Act to take reasonable steps to protect personal information. And there's been reference to various information standards or frameworks. So ISO 27001, which has been around for a very long time, has been discussed as well as the Australian Cyber Security Centre's Essential Eight, which is a very useful guide and framework that can be used as a starting point, certainly for smaller businesses.

Julian: One of the points of public discussion after some of these big breaches, I'm thinking of Optus and Medibank Private, was how many records, things like copies of drivers' licences, and passports, and those sorts of things companies keep. And I suppose that raised the question of whether information should be kept, particularly for a long time with former customers. How does that question play out in the context of legal practices where there are profession-specific record-keeping obligations?

Nitesh: Yeah, it's a very good question. It's something that's very much in the spotlight. Data retention obligations and data retention policies that businesses should have in place. It's a bit of a tricky question, it's trickier than you'd first think. Under the Privacy Act, there's already an obligation around personal information where, if you no longer have a need to hold particular personal information, then you've got an obligation to either de-identify it or delete it.

Now the question is, when is it the case that you no longer need to hold that information? The default position often is that there's a seven-year obligation under many pieces of

legislation that you need to hold records for seven years. There's also, under the Solicitors' Professional Conduct Rules, there's an obligation to hold client files for seven years. But the whole retention concept needs to be thought of in the context of, well, how do you protect yourself from claims and from scenarios that might arise out of legal advice you give, for example.

Julian: And things like ethical obligations to conflicts with former clients and the like, you need to know who those former clients are and that's an obligation which doesn't go away.

Nitesh: Exactly. And so, it's not as simple as, okay, well seven years have passed, we can now delete anything that's more than seven years old. Especially when it's for an ongoing client; you'd want to most likely hold everything you have in respect to that client to the extent that it's relevant for what you're doing now.

But let's talk about a scenario where you've provided a piece of advice to one of your clients. You've received your payment, that file is now closed at say June 2023. You would want to think about, well, yes you've got the seven-year obligation to hold the file, but when is it that a claim might potentially arise? You know, you never want to think about these things. But when is it that a claim might arise out of the provision of the advice you've given? When is your client going to rely on that advice? And then what is the limitation period that might come into force or that might apply?

Julian: And all of a sudden numbers higher than seven are occurring to me.

Nitesh: It could be that it's three years down the track since you provide your advice, for example, before that advice is relied on and then a loss is crystallised, and then a course of action arises, and then it's six years from there. So it could well be more than seven years. And you need to think about it from that perspective.

Julian: I mentioned the professional obligations of lawyers. Is there potential for cyber incidents and data breaches to lead to professional misconduct concerns for lawyers?

Nitesh: Look, it's an untested area and it's been subject to some discussions recently. It's probably worth highlighting a couple of key regulations that might have a role to play in all of this. You've got a duty to act in the best interests of your client, which I think is well known. You've got an obligation to provide clear and timely advice to assist a client during the course of a matter, and you've got an obligation to maintain a copy of client files for at least seven years after the completion of a matter, as we've just mentioned.

So these all become relevant when it comes to data breaches, but more significantly, more generally, around cyber incidents as well.

Look, professional misconduct findings are a very serious finding, and I would like to think that where a lawyer's taken some steps to address cyber risk and had regard to the solicitor obligations and rules and then suffers a cyber incident, that this wouldn't amount to a scenario of professional misconduct.

However, there can be extremes to this as well. And I could theoretically see a scenario where if a lawyer suffers multiple cyber incidents and has had no regard to protecting themselves or their clients from cyber risk, then yes, this might become a consideration because have you taken the proper steps to maintain a copy of client files for at least seven years? Are you really putting yourself in a position to make sure you provide clear and timely advice to a client without this kind of risk coming into play? So look, I could see it as a scenario but, at this stage, it's been really just discussions, but as this becomes further and further into the spotlight, yeah, we could see that.

Transcript

Data and Privacy Breaches

Julian: And I'd like to pick you up on something you mentioned earlier, we've talked about the obligation of the solicitor to act in the best interests of the client, but client expectations in terms of cyber security seem to be something that are changing quite a lot. In your observation, are clients' expectations a new source of pressure for how practitioners deal with cyber risk?

Nitesh: Yeah, absolutely. We ourselves have seen that from our clients, but generally the more sophisticated the client, the more likely you've already seen some additional obligations being imposed on you through service level agreements or otherwise.

So for example, if you have insurers, or financial institutions, or others who are regulated by APRA, they would be subject to Prudential Standard CPS 234, which imposes some pretty onerous obligations on those entities, and that includes having regard to their supply chain risk. They have an obligation to assess their information security, not just privacy, but information security having regard to the criticality and sensitivity of information. And again, there is an expectation that they consider what this means in terms of their supply chain.

So they are now imposing quite specific obligations on law firms who are providing them with services because we are part of their supply chain. And that goes then to the suppliers that we use as well, and so that's one example of how our obligations are being driven in some respects by what our clients are required to comply with and therefore our clients' expectations as well.

So that's with the APRA regulated entities. We've also got the critical infrastructure law reforms. We know the government has been taking a real close eye on what they need to do. They've been enhancing their policies and procedures and that, again, is being pushed down on their supply chain. When it comes to the smaller end of the spectrum, we'd expect to see a similar kind of drip feed eventually from them, and we are seeing that already, especially when it comes to the combination of scenarios where they've suffered a cyber incident and they're now making claims against the law firms.

Julian: With claims arising out of data breaches that affect law firms. Are there trends that you're seeing and things that listeners now should be aware of?

Nitesh: Yeah, absolutely. We've seen an increase in the claims against law firms arising out of data breaches and cyber incidents. And it's not just scenarios where it's very clear that the law firm itself has been compromised. In any scenario where there's been some sort of financial loss suffered by a client, they are pointing the finger at law firms. And in most of those circumstances what they are saying is that there's been a breach of retainer or a breach of duties of care owed by the law firm to them to mitigate cyber risk or have in place adequate cyber risk management. And so we expect to see more and more of that, and it's really important in those contexts that law firms have taken appropriate steps to protect themselves to deal with cyber risk, really, that's what it comes down to. If you haven't got the ability to demonstrate that you've taken the reasonable steps that are expected to address cyber risk, you leave yourself exposed.

Julian: It's probably worth mentioning the 2022 Federal Court decision of ASIC v RI Advice. Could you tell us what your sense is of the implications of that case?

Nitesh: Yes, it's a really good indication of where we're heading in all of this. It's a case that involves a financial services licensee and the decision was by the Federal Court of Australia in 2022. And so the court held that general risk management obligations under the Corporations Act that apply to RI Advice, required it to also have in place adequate cyber risk management and that it failed to do so.

That's the trend that we're seeing, that general risk management obligations include cyber risk management. And that again makes sense given that it's regularly seen as a top-five risk for most businesses. And that is increasingly what we're seeing, and that's seeping into what is expected around your duties of care. Now that still is an untested area of law, but I'd expect that no law firm wants to be the first test case when it comes to determining "Does having adequate cyber risk management, or mitigating cyber risk fall within the duties of care you owe to your clients?"

Julian: So you can't just search for the word cyber, but you've got to look at all your general obligations and think about how they might play out in the cyber context.

Nitesh: Yeah absolutely. It's a risk of how we conduct and provide professional services. We rely on email, we rely on electronic communications to provide the services we do, and so it needs to be properly addressed.

Julian: And that reliance itself poses challenges because when you're dealing with complicated technology, and all the technology that we have access to these days is actually very complicated underneath the hood. How do we deal with the question of, to what extent it's okay to rely on the experts and to what extent you really need to inform yourself and look under the hood yourself?

Nitesh: Yes. I mentioned earlier that it makes sense, especially for smaller law firms, but for law firms generally, I'd say to have a cyber security consultant or expert to come in and give you some assistance and guidance around what you should be having in place. But that is not sufficient. You need to have an understanding of what they're talking about, what they're recommending and what you need to do because ultimately it'll come on you to make sure that the recommendations are carried out, are executed. And again, there's a human element to all of this, and that includes every single practitioner, every single employee, and you need to make sure it's regularly reviewed.

One of the most common issues that we are seeing at the moment is a reliance on the existing IT provider. Now an IT provider in and of themselves might have cyber security expertise, but it's often the case that they are there to provide you with ad hoc IT services, especially at the small end of the scale when it comes to law firms, and that is a recipe for disaster. If you're relying on them to provide you with cyber security consultancy services or they're the point of contact to determine whether or not you've got in place adequate cyber risk management, it's not good enough. You really need to make sure, if you're relying on them, that they've got the proper qualifications and you properly engage them to provide the services that you need around identifying and putting in place adequate cyber risk management measures. Very regularly, it's the case that your smaller IT providers will not have in place the expertise or the qualifications to do that, but they'll give it a crack anyway. And it's really dangerous to be relying on that as a law firm.

Julian: So, it doesn't matter how much of a whizz-kid the teenage relative of one of the staff members is, they're probably not the go-to person for cyber risk.

Nitesh: Probably not. By all means use them to help you get up to speed, but in the context of having a proper cyber security advisor.

Julian: So you need to engage experts and have formal procedures. On the flip side of that, are there risks associated with the third-party service providers that you engage in this process?

Transcript

Data and Privacy Breaches

Nitesh: Yeah, so supply chain represents a major risk when it comes to cyber. We've seen a number of incidents already where service providers have had a cyber incident and that's impacted their entire client base, and that's included law firms on a number of occasions unfortunately. It's often the case that information that's held by these service providers will be found to be jointly held by their clients. So, for example, if you are relying on a human resources platform, if you've got an IT provider who manages your data, don't expect that they therefore hold all the risk when it comes to a data breach. It'll often be on you as well as your service provider. You need to undertake proper due diligence in that context. You need to understand what those service providers have in place to address cyber risk to protect you. You should request the ability to undertake regular audits and you should consider what obligations they owe you in the case of a cyber incident.

So do you have a say or do they have an obligation under the contract to inform you? Because it'll probably be more than just personal information we're talking about here. So you can't just simply rely on the Privacy Act. You should be looking beyond that, and you should be looking at what the contract says around their obligations to you in a cyber incident and then what remedies and recourse you might have as well.

That's a bit of a tip of the iceberg. There's generally a significant due diligence questionnaire that can come into play and other things. You should be getting your cyber security consultant to give you some guidance as to what you should be looking at in terms of your supply chain risk.

Julian: So, it's complicated and there is risk everywhere, but they're risks that legal professionals need to attend to. Nitesh, it's been great discussing these with you. Could we finish up with your main takeaway message for practitioners who are listening to us today?

Nitesh: The main takeaway here is that cyber risk is here to stay, and if you haven't already taken steps to address it, you should be doing it right now. No matter what size of business you are, no matter what size of law firm you are, cyber crime impacts almost all businesses and law firms are a lucrative target. The obligations are going to expand rather than contract. So again, be proactive, take the steps now to address the risk. You should also regularly review what you have in place. Just like any other risk management, you need to be regularly reviewing it. And you have to look beyond the technical protections. You need to address the human element, and make sure you know what you're going to do when an incident occurs, and that requires a properly tested incident response plan.

And from that perspective, when it comes to looking at cyber risk generally, I know that Lawcover have a significant volume of cyber resources available on their website, and they are a really good starting point to thinking about how you address this risk.

Julian: Nitesh Patel, thanks very much for speaking with us on Risk on Air.

Nitesh: A pleasure. Thank you.

Julian: Nitesh Patel is Cyber and Technology Principal at Gilchrist Connell.

Outro

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.