Podcast transcript: Cyber Security – More Than Just A Technology Risk with Susie Jones

**Heather:** You're listening to More Than Knowing the Law, the podcast that explores how to minimize risk through building good business culture and approaches, presented by the Legal Practitioners Liability Committee.

Hello, and welcome to More Than Knowing the Law! I'm Heather Hibberd, Chief Risk Manager at the Legal Practitioners Liability Committee. In this episode, we're focusing on cyber security risk in law firms.

If you're a practitioner that knows you should be doing more about cyber security, but think it's in the too-hard basket, or too-technical, then listen on, this podcast is for you. We'll demystify things like setting up two-factor authentication and updating your business software and you'll discover what you can do today to help make your firm more secure.

I'm joined today by Susie Jones, the CEO of Synch - an organization who partners with small businesses across a range of sectors, including law to improve their cyber security fitness. Susie sharpened her skills as the interface between technical information security personnel and senior business stakeholders.

Now, I think that means she was able to translate technical jargon for business people and vice-versa. Her specialty is in the people and process side of cyber security. As we began our conversation, she shared a story about what can happen when we aren't aware of what to look for when it comes to cyber security. Welcome, Susie.

**Susie:** Thank you for having me. A few years ago, I received a phone call from one of my close friends' mum who was in a similar industry, she was working on the other side of the law, in that she was a mortgage broker and had been working with a conveyance on a property settlement.

02:08 She had been chasing a conveyance of her information for a few days, and finally received an email just on Friday morning, as she's coming to the end of the week, wanting to finish everything and wrap everything up for the week. She double-clicked on an email, received a request to put in her username and password so that she could open the attachment, didn't think anything of it, and did it, and her phone rang and she went off and did a few things throughout the morning.

Two hours later, she started to receive phone calls from some of her clients saying, "You're sending me some strange emails, what's going on?" And she discovered that what had actually happened is that the conveyancer who she had been working with, they had had their credentials compromised and they had been lying in wait for the right opportunity to come across, they impersonated that conveyancer and sent my friends' mum this email, which then gave them, the cyber attacker, complete control over her computer.

So for two hours, in between when she put in her username and password and started receiving phone calls from her clients, they had had full access to all of her emails, all of that information that was saved on her clients and then had begun to send off their own attacks using her inbox to impersonate.

So then, it was several hours before she was able to find a way to lock them back out of her inbox, but in the meantime, that damage had been done. All of her clients then saw it as, not as her as a victim, but as her, as somebody that hadn't protected their data and it was many, many months of trying to unravel it and unpick the damage that had been done.

**Heather:** Wow, Susie, that sounds like a simple mistake that so many people could make, especially if you don't have any knowledge about cyber security. Despite our major focus on raising awareness of the importance of cyber security within the legal sector, we at LPLC are still seeing firms getting caught out in ways that could have easily been prevented with some basic safeguards.

Things like implementing basic cyber security measures such as MFA, multi-factor authentication and timely system updates, or understanding that you can't trust bank account details in emails and calling to confirm those details before they pay every time, as well as learning how to recognize scam emails.

It's led us to wonder why this is happening. Susie, you've been working with law firms for a while now, so what's your take on the extent of knowledge in the legal sector about cyber security? We have often had comments from practitioners who have been caught out by cyber security that they didn't think they would be a target because they're just a solo practitioner in the country or that they really don't have the big practice, so why would the cybercriminals look for them.

04:34 **Susie:** Absolutely, and it's a really common thought process of thinking that you're too small to fail or too small to be a target. The issue of course is that cybercriminals quite often are not targeting the individual, they literally don't care who you are, they target the technology, they target the assets and the value that you have in your business and who you are and what you do on a daily basis is neither here nor there to them. What they care about is what you have that they want.

And that's where that perception of, "Well, why would anybody target me?" is a real misunderstanding that we need to overcome because it has very little to do with who you are as an individual and much more to do with what information do you have access to, what funds do you have access to, what information on your clients do you have access to, and that quite often can be far more valuable than anything that you as an individual may have in your possession.

05:26 **Heather:** Which actually leads me to my next question, you've been working with law firms now for quite a while and your specialty is in the people and process side of cyber security. Do you think most people in the legal sector have a strong awareness of cyber security?

**Susie:** I think there's actually a very strong awareness of cyber-risk and that law firms are a target and that legal industry generally have a risk that needs to be managed. I think we're seeing a lot of, perhaps reticence to make changes that we believe need to be made. It comes from a lack of understanding of the responsibility that each individual person has when it comes to mitigating these types of attacks and risks.

It seems like such a big problem when we talk about cyber security, it sounds like such a big problem and that it's based in all of the technology, what could I possibly do to both improve our security or indeed how could just little old me be such a big risk to the firm? And I think that's actually where we need to break down the understanding or the misunderstanding, because personal responsibility is both the first line of defence, but also often the last line of defence for many legal firms.

06:39 **Heather:** So why do you think some lawyers and firms don't implement the basic cyber security measures that could save them from being caught?

**Susie:** I think there's a few reasons and we see this not just amongst legal professionals, but also other professionals in other white-collar industries, is particularly for those people that don't necessarily feel comfortable with technology generally, they don't want to look silly, they don't want to feel like they're silly.

And so when they're told to enable multi-factor authentication and they don't immediately know how to do that, the last thing they want to do is ask somebody for help or to be seen being silly and mess it up. So it's much easier to avoid. Unfortunately, that often leads to them looking like the ultimate silly person when they're then brought unstuck by an incident occurring.

So, I think we really need to overcome this whole perception that cyber security is very difficult to do, or very technical in nature, because if I was able to get my grandmother to install multi-factor authentication on her phone, then indeed, anybody can, particularly people in professions such as legal where they're clearly very smart people, they're the smartest of the smart.

So, being able to follow a few step-by-step instructions to put multi-factor on your email is not a difficult task. So I think that's one thing that is a barrier for many legal professionals and also very many legal firms. But secondly, also, it can just seem like such an onerous task, it can seem like something that's going to take forever, and when you're already working 16-hour days, that can feel pretty onerous to then spend some of your own personal time to implement some of these controls.

And I guess my response to that is that there is no reason why you can't implement a little bit of cyber security or a small cyber security control in as little as five minutes at a time. There are so many things that you can do that just don't take very long at all, but can make it that much harder for you to be brought unstuck by a cybercriminal targeting the technology that you're using.

08:29 **Heather:** And do you think that it's also not just the implementation, but once they've got it in place, they think it will be a hassle to use, the multi-factor authentication?

**Susie:** I definitely think so. There's a perception and it comes from very valid roots, that any time you implement something that makes you more secure, you're taking away some flexibility or some capability that you previously had. And it's very true that there is to a certain extent a juxtaposition between flexibility or collaboration and security.

But I guess it also comes down to, well, really, what's got the bigger issue behind it? Is it more important for you to be able to access your emails in 10 seconds, than it is in 30 seconds, if it means that anybody could access your email in 10 seconds instead of only you being able to access it in 30 seconds?

Particularly, these days, most security controls, security firms have spent millions and millions of dollars investing into the ease of use. So, to make security controls so much easier to implement on a daily basis.

Many of those excuses simply don't exist anymore. It also can be the case that sometimes using one control like multi-factor authentication may add a few extra steps or a couple of extra seconds to a step, but that can also be counteracted by using another security control.

09:49 So one example is using password managers. So password manager is a piece of software which acts as a safe or a vault for all of your passwords. It means that the only passwords you need to remember is the password to get into your password manager, but it also means you can use very strong, unique passwords across every different account that you have.

And the best thing about using password managers is that it will autofill the password into any account that you're logging into, so that saves you those few seconds. So if you're using a password manager, you can take those extra seconds that you would've spent going, "Hm, what's my password to this account?" And actually spend that time using multi-factor authentication and then not only do you have two of the strongest controls to stop anybody from stealing your username and password, but it can be a lot more enjoyable not having to think, "What password did I set for this account?"

10:36 **Heather:** The other thing I was wondering about is do you need multi-factor authentication every time you log in? Clearly, it would possibly be more secure, but is there a halfway house of having multi-factor authentication on a new device?

**Susie:** Absolutely. So, many, many different pieces of software or devices will have a "Keep me logged in for 7 days", or 10 days, or 30 days, and so I know on my own work computer, I have various different accounts that I log into, say once a week, but I will have the box checked to say, "Keep me logged in for this week." So that if I do go back into it tomorrow, I don't have to do the multi-factor again.

However, if it is a week or two before I log in again, I will and that's definitely a halfway point between the two. The point of multi-factor authentication is not to make anybody's day more difficult or to slow anybody down, it is literally just to stop people from being used compromised password and username to get into somewhere where they're not meant to get into.

11:33 **Heather:** Because we know that the cybercriminals are able to get ahold of your password in lots of different ways, through brute-force attacks and through fishing emails and even buying passwords off the dark web, if you've used the same password for multiple accounts. And the whole point of multi-factor authentication is to prevent them from getting in once they've got your passwords.

**Susie:** Exactly right, and it's also really important to think that it doesn't always need to be a code sent to your phone, it can also be a code in an authentication app which you can also then quickly copy across between different applications on your phone, etc.

There's been many, many instances where we've seen people fall victim to a cyberattack, where their email has been taken over, essentially because they've used the same password for their email as they have for say, LinkedIn. LinkedIn have had several very well-known data breaches over the past decade or so and when you use the same password across multiple spaces, it really doesn't take any effort whatsoever for a cybercriminal to get your username, then your email address, that password and see if it works.

12:39 If that's the case, let's think of it as you losing your keys, you know that somebody out there has the keys to your house, but instead of changing the locks, you go, "Well, maybe they don't know where I live." It's not the best approach to security. In that case, if you know that you've lost your keys, or in fact, if you know that somebody has taken a copy of your keys, then you change the locks and that's why you should always change your password in this.

Similarly, you have an alarm, and you can think of the multi-factor authentication as being that alarm as well as the locks on the door to your business.

**Heather:** That's a good analogy I think. So what are the barriers and how can we overcome this lack of appreciation of what they really need to do and understand that it's easy to do, do you think?

**Susie:** I think there's a few things. First of all, taking a reminder that it's not about your technology, and it's not just going to be a hassle if you fall victim, it's going to be incredibly embarrassing. Needing to admit that the whole reason why your firm has come unstuck by a ransomware attack that's brought everybody down or that your client's information is now in the hands of the wrong people because you did nothing to protect that information stored on your system, that can very quickly become one of the most embarrassing conversations of your working life.

13:48 So, knowing that all you need to do to avoid that embarrassment is to enable multi-factor authentication or buy a password manager, I think that's one way of thinking, you know what? That's a pretty easy and quick way for me to avoid having to admit that I just knew what I was meant to do and I just didn't do it.

There's not too many aspects of anybody in the legal profession's life where they could say, "No, I knew that was what I was meant to do, and I just chose not to do it." So I'm not quite sure why cyber security and the technology aspect is still an area where this is quite a pervasive behaviour that we're seeing.

Think of it as just like every other control that you in your business and your organization have in place to protect the information of your clients, protect your organization, think of it as exactly the same thing. It's definitely going to be a very embarrassing conversation if you've been told to enable multi-factor, you haven't, and then you come unstuck.

14:42 **Heather:** And I can tell you from the claims that we've had, it also means that if money has gone missing, the client doesn't have the money to settle their purchase, and that's a very stressful situation for the lawyer to be in.

Or if they've discovered that their email has been hacked and in one situation, the cybercriminals had been sitting in there for about a month and had siphoned off over 200 emails and the law firm had to spend a considerable amount of time trying to track down all of the settlements they had coming up to make sure that all of the payment details were correct.

And six weeks after that, they still had one matter where they payment was paid to the wrong account, so the principal in that case had many sleepless nights trying to manage the fallout from that email compromise.

15:32 **Susie:** We're also starting to see ASIC sitting up and paying a lot more attention to organisations that repeatedly don't heed the advice to secure their systems. So, there was an example last year of RI Advice which was a financial services and mortgage broking organization that had several data breaches over the course of a period of time and didn't take what most people would say were reasonable steps to resolve those issues, to improve the security and they kept falling victim.

And ASIC actually sued them last year. So, we're starting to see the government authorities and agencies sitting up and paying far more attention and if you're not able to demonstrate that you've taken appropriate steps, that you have met your obligations under the privacy principles, then we can only expect to see not just sleepless nights, but potentially pretty hefty fines and enforceable undertakings heading your way as well.

16:21 **Heather:** Firms who have IT support, should they be contacting their IT provider and asking them to implement multi-factor authentication and making sure that that happens, is that the best advice do you think?

**Susie:** The important thing to think about is that cyber risk, as much as it's quite often called IT risk or cyber risk, it's not only a technology risk, it's actually a whole of business risk, so it's really important that IT divisions and teams work alongside the likes of the HR team to make sure there's appropriate training being provided on how to conduct your work and share files safely and securely.

How to actually access your email remotely using multi-factor authentication as well as the tech teams actually being on the back end, enforcing it, so that you don't have a choice and you can't access things unless you have these sorts of controls in place.

So it's about combining the people aspects, the process aspects and the technology aspects into all of it so that you can protect all of your business, not just the technology, because as I said earlier, the people can be both the first line of defence, as well as the last line of defence. It's certainly not always about technology.

17:29 **Heather:** We've had firms say, "But I have good cyber security software and I update my systems regularly, how could this have happened?" But it was somebody clicking on a link and allowing the cybercriminals in, so yeah, that's a really good point. So what are your top four things that you think people can easily implement to make a difference in this space?

**Susie:** I think the first thing that I would recommend everybody do after listening to this podcast is, go to their laptop or their computer and restart it, and install any updates that are sitting there waiting for you to actually install. So often we talk about patching your computers, etc, but often it doesn't happen if you never actually turn your computer off.

Al you ever do at the end of the day is make it go to sleep and then you start it in the morning so that you don't have to restart the whole thing. Then those updates don't get on to your computer as quick as they should be. So everybody, just go and restart your computer and allow any updates to install.

Secondly, enable multi-factor authentication on your email. I can guarantee you it won't be any more than about four clicks. And they will make it so, so simple for you to do it these days, so make sure that that's in place.

And for those of you that already do have it enabled on your email, enable it on something else. We all have multiple accounts to multiple bits of software that we use these days, so slowly, but surely, just enable it on everything that you can.

The next thing, buy a password manager, and set it up and use it. Stop using "password123", or "Iloveholidays", or your son's name followed by you know, 1947, 1948, 1949. Use the software that is designed to keep your password safe, and make it easier for you to log in wherever you need to.

19:03 And then finally, given so many others are now working in a hybrid situation between offices and working from home, make sure that you actually have a separate network set up for any work that you do for work, than you do for at home.

The last thing you want is for you to be working on incredibly sensitive client data and files on the same network with the kids' Netflix or schools or Fortnite game it is on, so that can sometimes be a little bit tricky, but while YouTube is a wonderful place that has a lot of information on how to set up these kinds of accounts, most modems will allow you to have two separate networks set up.

So that's one thing you do on the weekend and particularly for those people that are in lockdown across Australia now, we've all got a little bit more time up our sleeve, so if that's one of your weekend chores, is to figure out how to set up separate networks across your work and home, I highly recommend that for everyone.

**Heather:** I was just reflecting, with the password manager, we have had questions from people about how secure are they if you've got effectively all your eggs in one basket? Is that a good thing to do? Can you re-assure people that they are secure?

20:07 **Susie:** Absolutely. So, this is one of the questions that comes up regularly and it's completely a fair question. So first of all, the password-management software is only going to be strong and secure provided that you use a password to get into that software that is strong and secure. So if you only remember one password, make sure that it is a long one, it is unique.

So I know my password to get into my password manager is about 25 different characters long. But it's the only password that I remember, because everything else is in my password manager. So took me a little while, I have a passphrase that reminds me of what it is, but that means that I can be assured that nobody can guess my password and get in there.

I think it comes down to, these companies are absolutely invested in the security of your password. Their only reason for existing a lot of the time is to secure your password, that's the kind of company that I want protecting my password, rather than any mental algorithm that I could come up with to create a unique password across the 400 different accounts that I have.

So it comes down to, they can be trusted, it's better than anything that you can probably make up in your own mind and it's certainly gonna be better than having a spreadsheet full of passwords that anybody could stumble across.

21:17 **Heather:** The other simple thing that we've been saying in our messaging is to check your email rules. Is that something that you've seen as well? That once the cybercriminals get in, they set up a whole lot of email rules to take the emails out of your system? Can you talk about how people might do that? How they can check their email rules?

**Susie:** Yeah, absolutely and it doesn't need to be something you check every day, maybe not even every week, but I would recommend certain things that you do, say on the 1st of every month and checking your email rules would be one of them.

So it's normally very simple, you go into the settings in whatever your system is that you're looking for, find where it says rules and make sure there is no rules in there that you haven't set up. So the ones that would typically be there would be ones like automatically forwarding on certain emails to an inbox. Automatically deleting emails from your inbox, automatically deleting emails from your sent box.

Because if they're impersonating you and sending emails on your behalf, they will delete them from your sent box so that you can't see they're over there. They are the kinds of rules that are regularly put in place by cybercriminals to hide what they're doing within your inbox and if you never check to see the rules are there, you may never know that they're there, because they're actually designed to keep these things hidden.

So just getting into a regular rhythm of checking those things, about once a month can be a really good habit. And the good thing is, is that if nothing has happened to your inbox, that job will take about 30 seconds to do and then you can get on with your day.

22:37 **Heather:** We talked before about brute-force attacks, can you explain how they work?

**Susie:** Absolutely, so I mean, brute-force attacks, it really is as you would imagine, the technology version of the term, right? So it is using computer software to just try thousand and one different passwords one after the other, after the other, after the other until it hits one that is correct. So we all know the jokes around using passwords like "password123" or "welcome1" and all of those typical ones.

The brute-force attack is where they will set up a computer program to just keep trying to get access to your inbox over and over again until they get in. So that's why you'll find many services will have things like, "You've tried too many times, you're now locked out until you can try again." That is to avoid things like forced attacks.

What's interesting about the legal industry and profession is I was reading the most recent report from the office of the Australia Information Commission and brute-force attacks are actually not the most common within the legal industry. The most common type of cyberattacks come down to fishing or credential harvesting, which is basically stealing your username and password.

23:42 So, it says to me that cybercriminals find that when it comes to the legal industry, the best form of attack is the one that is taking advantage of poor behaviours by the people within the industry, rather than the technology itself. So just by making a few behavioural changes, you're going to protect yourself so much more knowing that those kinds of attacks are not ones that will be successful against you.

**Heather:** And does that mean that we should be having regular cyber-training or cyber-reminders for our staff? Is that a good way to go about it?

**Susie:** Absolutely. I think just like anything, we need to have regular reminders to keep it front of mind. So if you think about 30-40 years ago, how did Australia overcome so many workforce injuries when it came to work, health and safety? It was from regular training, it was from enforcing training, it was from having posters around, it was from having toolbox talks, it was from implementing things like when a new lawyer starts in a new office, they need to have an OHS check of the way that the posture is for their desk chair.

These sorts of things were introduced to avoid physical harm being so prevalent across workplaces 30-40 years ago and that's exactly the sort of change that we need to be able to stop, those intangible injuries occurring to businesses and people. It's keeping it front of mind particularly when the best-case scenario, if you're doing everything right when it comes to cyber security, then nothing happens. So the best way to keep it front of mind is to keep talking about it.

25:06 **Heather:** Good advice. That comment really ties back, Susie, with what you were saying at the start, about people taking more personal responsibility for cyber security.

**Susie:** Yeah. Certainly, in the past, we've heard many people anecdotally saying things like, "Well, cyber security, that's not my job, that's the IT, the IT crew's job." Or, "Surely, I work for this large firm, they must have things in place to stop these sorts of emails or attacks getting through. The unfortunate reality is that there is no silver bullet.

There is no single technology control that an organization can put in place that will forever stop these sorts of attacks making it through. There's no single piece of technology that could be installed on your computer that could stop you from double-clicking on a link that you really and truly know is dodgy and you shouldn't click on.

It all comes down to each and every one of us needs to take some personal responsibility and really think about how am I behaving in a way that supports the company to remain secure rather than undermine those security controls that they've put in place.

26:09 I think it's also another thing that everybody could take away and consider what is one thing that I could do that my company couldn't necessarily see me do that might undermine the security of my business, as something as simple as re-using the same password across all of my accounts is something that your organization may very well not know that you're doing, and yet you know that that is undermining the security of everything that you work on.

It is nobody else's fault, it is nobody else's responsibility other than your own to make sure you're using different passwords when you've been told that that is the only way to keep people out. So it's these kinds of mind shifts or shifts in mindset that we need to really put in place because the absolute best way for you to avoid falling victim to a cyber-attack is for you to remain vigilant yourself, for you to share potential attacks, if you receive a fishing email, are you reporting it to your IT team? Are you telling anybody else so that they can avoid falling victim to the same attack?

It's not quite enough these days to just not fall victim yourself, it's also about sharing the experience and the knowledge that you have with others, which not only encourages them to do the right thing as well, but also helps them to learn from your own lessons that you've learned along the way.

27:20 **Heather:** Well, thank you very much Susie, that's been a fascinating discussion and I hope our audience have taken away lots of good tips on how to be more cyber-safe in the future. Thank you.

**Susie:** Thank you.

**Heather:** Thanks so much to Susie for sharing her guidance with us. To summarize, the key takeaways from this episode, cybercriminals target what you have of value, not who you are. So, most law firms are targets irrespective of size. Multi-factor authentication is not hard to implement, but the potential consequences of not having it far outweigh the time it takes to set it up and utilize it.

To connect with Susie and discover more resources on this topic, visit the shownotes. Link is in the description of this episode.

You have been listening to More Than Knowing the Law. And I'm Heather Hibberd. If you would like more information about the topics we have discussed today and links to helpful resources to manage your risk, visit lplc.com.au/podcast.