YS UP GOVERNANCE AND BOARDS PODCAST

Episode 24 – Cyber Part 3 - Data Protection, Privacy and Information Technology with Alex Hutchens

Transcript

Intro:

Welcome to YS Up Governance and Boards podcast brought to you by 3YS Owls Governance Consultants. Covering hot topics in governance, risk. latest regulatory changes and issues keeping directors and executives awake at night. Here are your hosts Ainslie Cunningham and Deb Anderson.

Deb Anderson:

Welcome to today's episode of YS Up. Today we are joined by Alex Hutchens. Alex is a Partner and Head of Technology, Media, and Telecommunications Industry Group at McCullough Robertson. His key practice areas are data protection and privacy, information technology, and telecommunications. In that role, he advises clients extensively on cybersecurity and data protection matters, particularly in connection with the rollout of new technologies, the mobilisation of workforces, and reporting and responding to data breaches. Welcome, Alex.

Alex Hutchens:

Good morning. Thanks for having me.

Ainslie Cunningham:

So, tell us a little bit about Alex Hutchens and how you've wound up here?

Alex Hutchens:

It's not a very exciting story, I'm sorry to tell you. When I was at law school, I took a real interest in the internet, which was very new and developing at the time, which tells you a little bit about how old I am. And at the time, it was really the thing that interested people was the power of being able to share files and be connected globally, and you could repeat the same thing many, many times without losing any quality. And so, copyright and sort of protection of rights was a really big deal.

Alex Hutchens:

And as we've grown through that time and seen the internet expand into, not just connected systems, but now wireless systems, and we move into 5G, everything is connected, everything can be shared and distributed. And not only has that brought benefits, but it's obviously brought risks with it as well. And so, from that very early point, I've kind of had a real interest in this intersection of law and technology and how it's changing our lives quite rapidly. And so, I've just really followed that path ever since I started practicing as a lawyer, I've always been connected with that industry and work in this space a little bit. And it's just kind of grown from there. So, it's a really boring backstory. I'd make a terrible film character.

Ainslie Cunningham:

No, and in industry, I guess too, that's still relatively young compared to traditional financial or accounting or legal backgrounds. Cybersecurity is something that's actually relatively immature in that sense.

Alex Hutchens:

Look, absolutely right. Some of the legislation that's trying to deal with these issues is 30 or 50 or more years old. And not only was this kind of thing not even conceived of, it certainly wasn't addressed in the legislation or the legislation wasn't crafted in a way that's very flexibly able to be applied to this. So, that's that real challenge. This is so new, and things are moving so fast that the law is, as ever, playing catch up, and there's some tensions there. It's really obvious that things just aren't quite from a regulatory setting perspective ready to deal with the issues that we're facing day to day.

Ainslie Cunningham:

Yeah, square peg, round hold scenario by the sounds of it.

Alex Hutchens:

Precisely. Yeah.

Ainslie Cunningham:

So, tell us a bit, some of the things that might be keeping directors and executives awake at night in the cybersecurity space.

Alex Hutchens:

Look, I think the ever present threat of some sort of cybersecurity incident is what's keeping directors awake at the moment. And indeed, everyone throughout management teams and professional services teams alike. It is just, I think, the reality that in the modern world with all of our systems and all of our workforces so connected, that there are so many potential threat vectors, if I can use a really sort of ugly industry term. But there are so many potential points of attack and so many weaknesses that I think everyone in management really is just waiting for the call to say that there has been some sort of cybersecurity incident, whether it be privacy related, to do with personal information, or whether it be to do with corporate information, you know?

Alex Hutchens:

The secret formula, the secret sauce has somehow been compromised, that sort of cybersecurity incident, or a ransomware attack, where systems are compromised and functionality has been shut down as a result of that, and threats are being made that systems won't be put online again unless a ransom is paid. That sort of thing is almost inevitable now. I think the cliché that it's a matter of if not when. And everyone in management, I think, is thinking about that. And if they're not, they certainly should be.

Ainslie Cunningham:

And how are organisations dealing with say ransomware attacks?

Alex Hutchens:

Look, specifically with ransomware attacks, there are a couple of schools of thought around this. One is pay the ransom and cross your fingers and hope for the best and hope that whoever it is who's locked up your system will be good to their word, their digital word and unlock your system again. So, that's typically how it works, you know? That's the sort of nightmare scenario. You boot up your computer, and instead of the login screen, a message splashes across to say, "Your system's been locked, and you need to pay this many Bitcoin to unlock it." And if you do, it will be unlocked. And so, there is a school of thought that you can do that and things will work. It's a kind of business model, a recognised business model. If the ransomware attackers didn't then unlock the system, that threat's no longer going to result in money being paid, because people will soon learn that if you pay, you still lose your system, so there's no point in paying.

Alex Hutchens:

There's another philosophy, of course, which is, you don't pay, and you try and solve the problem and unlock the systems yourself. This can be a really, really difficult thing to do, time consuming, technically difficult, very expensive. But there are obviously many principles at play here, and

people don't like to respond to ransomware. So, ransomware, specifically kind of plays out in a couple of very distinct ways depending on that philosophy.

Deb Anderson:

And are spear phishing attacks still quite prevalent?

Alex Hutchens:

Absolutely. So, spear phishing is actually one of the most common attacks that we see today. And the reason behind that is it's a form of social engineering. And I'll explain what that is in a second. But it's a form of social engineering, which enables attackers to get access to other information, which might then be more useful from a cybersecurity perspective. So, there's a very famous now white hat hacker called Kevin Mitnick. And he used to be, back in the 80s, one of the FBI's most wanted people, such were his skills in penetrating IT networks. But he is now on the speaking circuit and shares stories and writes books about the types of things that he does when he consults to companies to harden their systems.

Alex Hutchens:

But one of the things he talks about is that individuals are still the weakest link. It's the human factor that really is the best way into a system. So, you can have all sorts of IT protections. But if people still set their password as welcome1, or as password, or if they put up on social media their pets names and their birthdays and their first share house address and all of those usual questions that you get to prompt when you forget your password, if that sort of information can be gleaned, then you can use that to obtain access to other systems where you don't have the proper credentials. And so, spear phishing is really about not just blanket attacks, but quite targeted attacks, understanding that a particular person, it might be an IT manager, it might be a CEO, someone who's got very highly credentialed permissions within an IT system. If you can compromise them personally, get their information then perhaps you can then log in as them and exercise those credentials or pretend to be them and force other people to divulge information.

Alex Hutchens:

And so, a classic threat that we're seeing now is if a CEO's email is compromised, that email account is then used to send a very demanding email to the finance team saying, "We're late on this account. You need to pay this immediately, here are the details." And of course, the CEO has no idea that email is being sent. And the finance people will, of course, do immediately as they're told by their CEO. And that account will be an account linked to the attackers, and off they get with the money. So, that's one of those things where, if you can compromise an individual through very targeted attacks, then you have a very good chance of compromising broader systems, which is then the real outcome that is being sought there.

Ainslie Cunningham:

And so, are you seeing businesses who may be targeted in this space in terms of ransomware, are they actually paying the money?

Alex Hutchens:

Yes. Look, I have seen it done, or I know that people have done that. And to be perfectly honest, that is why the attack works and the model works. The easiest way through to have your systems unencrypted, decrypted and unlocked is to pay the ransom. That's the deal, and you get it back. And there are reports that that does actually worked. And, as I mentioned earlier, that's the business model. If it didn't work, I guess very quickly that would cease to be an effective attack. Although, law enforcement in particular is not particularly keen on that approach, because it does, of course, make it a more effective business model and probably will lead to greater prevalence. So, there is, I think no absolute right or wrong there. But people do pay. I've certainly heard of that happening.

Ainslie Cunningham:

And are you still seeing attacks from, say malware being installed through USBs laying around? Or is that becoming a bit redundant now and it's more wireless?

Deb Anderson:

Too many people have had that test done on them.

Alex Hutchens:

Certainly, the compromised USB is a cybersecurity professional's worst nightmare, because if you think about the number of devices we have now just in our personal possession, and then you multiply that across a whole organisation, there are all sorts of ... They all become individual points of vulnerability. And if you can get a USB inserted into one of those USB ports with some malware on there, then you can get access to the whole system and do all sorts of things. You can install listening devices, which then start crawling around and waiting for people to type in passwords, and they can just watch network traffic and understand what happens within that organisation and try and determine a great way to attack it.

Alex Hutchens:

There's a report, I believe, and I have no reason not to believe it, although I imagine because it's part of sort of state security, it would be partly contentious. But there is a report of a virus or malware called Stuxnet, which was originally promulgated by the US security services. And reportedly, it was used in an attack on an Iranian nuclear reactor several years ago now. And basically, the vector through which that was brought in was an individual who worked in that nuclear reactor was compromised or working with the US, and managed to, through a USB port, introduce a compromised USB device, which then deployed some code into the system, and then affected the system so it would overheat and meltdown. And so that led to sort of physical destruction through the introduction of malware code.

Alex Hutchens:

Now, that's obviously a very different scenario from what most businesses are dealing with. But it's a really great example of how those USB ports are really still a major vulnerability. And as a result of that, a lot of organisations in fact disable USB ports on work dispensed laptops. They'll say, "We don't need that. We will manage all of our software installation centrally. You just don't need those USB ports. They're just too great a vulnerability." But I should say, with the evolution of wireless technologies and connected devices, it's not only through that sort of infected or compromised USB device that malware can be introduced, there's all sorts of ways now. Open WiFi networks are another great example of a way into devices.

Ainslie Cunningham:

Yeah, for sure. And I think you've briefly touched on it before, Alex, about with Kevin Mitnick and the human element still being the weakest link in organisations. So, from a risk mitigation perspective is training of those staff still the greatest form of risk management?

Alex Hutchens:

Look, I think so. Awareness is such a powerful tool here, because people operate through habit, particularly in current circumstances, where not only are they trying to do their job, but they're doing it in compromised circumstances from home, and they're also trying to homeschool their kids and have everything else going on as well. Quite often, people are distracted when they're doing things and interfacing with their devices. And so, if they have good habits, they'll just default to doing things the right way. And so, if they see an email with, for instance, a hyperlink in it, they'll think, "That's suspicious. I've been trained on not clicking on links in emails." And everyone has heard that.

Alex Hutchens:

But quite often, if you are distracted and you've got a few things going on, if that's not fully ingrained and habitual, that's the sort of time when people are most vulnerable to making a mistake or stepping outside of that best practice. And so, I think not only training staff, but updating that training and doing it regularly so that it reinforces the message. And also update it to reflect any new threats that are being seen, because this is such an evolving space, you know? Every 12 months there is a slightly different thing or a new trend that we're seeing. And it's a great

opportunity to, as I say, reinforce the message, but also update awareness to be aligned with current practices.

Ainslie Cunningham:

Yeah, absolutely.

Deb Anderson:

So, are there any new forms of cyber-attack that are sort of emanating?

Alex Hutchens:

I mean, look, yes there are. And I think the best example of that is, we've seen the Prime Minister and other senior government ministers come out in the last couple of months talking about the threat of state sponsored actors. And that the number of attacks and the sort of vectors through which those attacks are being made are increasing and changing. So, I think the spear phishing ... I think the thing to note is that the social engineering component is getting so advanced that the spear phishing attacks are becoming really, really believable and much more sophisticated. Long gone are the days where a logo is sort of snipped out of somewhere and pasted in roughly and then there's typos and different fonts and things.

Alex Hutchens:

The thing about spear phishing is now people are being targeted on their own habits and their own personal behaviour, be it online or in the real world. They're kind of being tracked and monitored. And then the right message is being crafted to really hit a vulnerability. And so, I think that's still a really prevalent example and an evolving one. We're seeing a lot of COVID related scams as well. So, particularly with people being on JobKeeper and JobSeeker and there are repayment holidays on loans. And all of those things mean that people are expecting to have conversations with government agencies and their home loan provider and other major corporates.

Alex Hutchens:

And so, we're seeing a lot of messages trying to pick up on that dynamic, and threatening people, "You're late on your loan," or, "You didn't fill out the loan waiver application properly. You need to call us straight away," or, "You owe us this money and you must pay us immediately." And so, because people are expecting that government intervention and that strange interaction with the large corporates, and because these are unchartered times, there's not really a well-known process for this. This is quite often the first time any of us has been dealing with this sort of thing. Then, that kind of uncertainty is ripe for the picking. So, I think a lot of those COVID related scams are probably the real emerging threat and the large volume of threat that we didn't see 12 months ago, for instance.

Deb Anderson:

Just generally working from home and not having the same sort of security in place as well.

Alex Hutchens:

Precisely. People are connecting to devices through their home WiFi networks. They might not be as secure as the corporate network that they plug into when they're in the office. So, that's an example. People are more lax about even just physical security. So, if they might be reviewing a report at home or looking at the quarterly numbers or something, and they print them out to scribble notes. And then they just throw them out into the general domestic rubbish, you know? Those sorts of things would normally go into secure destruction or into a shredder or something like that. So, it's not even a cyber threat as such, it's a real-world threat.

Alex Hutchens:

But as you say, working from home is just a different environment, where people don't have the same resources available to them, so cut corners. And also aren't necessarily thinking in quite the same way, you know? They're thinking about making dinner and they're typing an email to the boss urgently at the same time. They're not really in work mode. And that's a real problem from a cybersecurity perspective. It's the reality, and it's no criticism of everyone. We all have to work that

way. But it's really worth being aware that that's a totally different dynamic, and one where there are new threats.

Ainslie Cunningham:

Yeah, and I think too for organisations that don't have a lot of resources in the first place, like for large IT teams, large legal teams, that sort of stuff, to actually manage some of these challenges, it's even more difficult for those organisations to, one, know where to find the information in the first place. And two, then how do we manage it and deal with it and kind of get a little bit of a risk framework in place. So, what are the sorts of things that sort of the SMEs can be doing in this space?

Alex Hutchens:

Yeah. And look, I agree with you 100%. It's the smaller organisations who really now just have yet another thing they need to be expert in that just really ... It truly is relentless. So, I think one of the things that permeates all of the sort of best practice guides around cybersecurity is to understand what your environment is and where the perimeter is, so that you can then put the appropriate perimeter protections in place. So, that's really about understanding, what is the infrastructure we have in the office? What are the devices people have in their hands? What are the systems we use? And what then are the obvious vulnerabilities? So, if you've got a mobile workforce whom you've given mobile devices to, they should all have password protection on them, so that if they're lost on the train, at least there is a barrier there, because a lot of important information is stolen on them.

Alex Hutchens:

If you've got a corporate network installed in your premises, obviously you should have a firewall set up for that. If you used a lot of cloud based systems, you can get a lot of security inbuilt into those or wrapped around those probably is the better way to say it, through your provider. So, understanding that, yes, I'm storing things up in the cloud, and that's a potential vulnerability. What am I doing with my provider around security there? Because there are different levels of security you can get based on how much you're willing to pay and what sort of sensitivity of information you have.

Alex Hutchens:

So, I think understanding those elements of your system mean that you can then identify the risks and address them. And it doesn't mean that you have to address all of them or you have to have the gold standard everywhere, but different things will be more important and less important for different businesses. So, unless you have that understanding, you just can't begin to answer the question. And I think talking to your staff about these issues, it can be formal training, if you've got the resources for that. But equally, if you're a much smaller organisation, the beauty of that is you have a much more direct connection with a higher proportion of your staff. And so, you can talk to them, you know The staff meeting is a great forum to talk about cybersecurity issues, see what people might be seeing in their personal lives, any issues they're seeing working from home and how they might catch themselves cutting corners or seeing problems arising. There's a degree of flexibility there which can actually become a strength as well.

Alex Hutchens:

And I guess, finally as well, there are some really good resources out there now. If you are hearing some of this and think, "Well, I don't even know where to start. I'm really not an IT person. And some of these terms don't even mean anything to me," things like the Australian Cyber Security Centre, the ACSC is becoming much more active around education, I'm finding in the last 12 to 24 months and beyond. It's producing reports and publishing materials, which are really helpful to set up frameworks and best practice kind of behaviours. And so, it's worth, as a jumping off point, going to something like Australian Cyber Security Centre's website would be a great place to start.

Alex Hutchens:

Yeah, they are a good resource, aren't they?

Alex Hutchens:

They really are. They really are. As I say, been around for a long time, but do seem to be shifting, I think, to really be much more visible and supportive of people in the marketplace who need to learn some of this stuff, which is really foreign to some people. So yeah, they're a great place to start.

Deb Anderson:

So, some tips, Alex, in terms of choosing passwords? Obviously a lot of people use the names of animals and children.

Alex Hutchens:

I know there's quite a few sort of password programs that you can buy. But in terms of choosing something that's easy to remember yourself, what are some tips?

Alex Hutchens:

Well, look-

Alex Hutchens:

Without giving out your password.

Alex Hutchens:

Yeah, I'm trying very hard not to give out any of my usual ones. We've all go the usual ones. I mean, look, using a password manager is by far the best way, because you don't even know what it is. It's kind of stored securely and it's really unguessable. And yes, of course, you face the problem that you can't remember it. But if you've got your system set up properly, that will be secure enough to get you in and no one else. In terms of actually choosing one that means something to you, there are ... We were talking about social engineering before. And one of the things is, if people understand who your kids are or where you live, what football team you support, whatever it is, those things are kind of guides into, "Well, how can we start trying to force our way into your system by guessing passwords?" So, this sort of brute force attack comes from social engineering, they're educated guesses.

Alex Hutchens:

But then, other brute force attacks just run ... Every word in the dictionary can be run into a password field to see if that will work. And so, using sentences rather than individual words is a great way to do it because that's not so susceptible to that brute force attack, it's adding to the complexity. Of course, using different characters. So, sometimes you can switch, almost like you're texting or trying to look like an energy drink or something, where you swap characters for letters, so they sort of look the same, and you know the word, but they're a bit different, can be another way to go about it. And not reusing the same password across multiple platforms is important, because again, going to the social engineering point, if they've managed to crack into one of your accounts, then that password will be the first one that gets tried across every other account.

Alex Hutchens:

And if your, for instance, email has been compromised, it will be easy to tell which service providers you interface with. And so, it will be possible to start checking all of those with the password that's been compromised. And so, really not reusing the same password is critically important, because once that gets out, likely it will be tried on so many other of your presences online.

Ainslie Cunningham:

Yeah, good tips. And so, all these things have failed, and you've now suffered a data breach. Where to from here? First steps, all the bits in between.

Alex Hutchens:

It's the phone call everyone dreads getting. Ideally, you will already have had a data breach response plan put together. And one of these plans really does what it says on the label. Once you

have a compromise or a suspected compromise in your system, you then follow the steps. And so, that sort of plan should set out who it is in your organisation who's going to take responsibility for leading the response for conducting investigations. So, you might have the IT people trying to work out, "All right, what's happened with their systems?" And you might have the coms people saying, "All right. Well, how are we going to deal with it if the press starts ringing us or customers start complaining?" You may have lawyers thinking about which regulators you need to deal with. You will have senior decision makers who can say, "Well, understanding all of this informamtion that's come back, here's what we're going to do." So, that is the ideal response. And that, of course, requires some planning in advance.

Alex Hutchens:

And again, particularly for smaller businesses, that is a degree of sophistication and almost a luxury that many can't afford. And so, you'll be caught without that. The first thing I would do is try to get a handle on what has happened. And if you need to get ... This will almost certainly involve some sort of IT assessment. So, if you don't have in-house IT capability, I would be trying to get a cybersecurity response person. And you can Google them now. It's one of the fastest growing jobs in the world, I think. You can Google them and find them. And they will come in and do some forensic work to work out what systems were compromised, when, has data been exfiltrated or not? If so, what was it? What other unusual activity has happened on your network? Have passwords been used to try and log into other accounts? Or have administrator privileges been found? And is there now some strange activity on the network as a result of that?

Alex Hutchens:

So, trying to get a handle on it is the really most important thing, because again, you can't respond unless you know what it is you're responding to. Coming back to the cybersecurity centre, they are very involved with industry and have, for a long time, encouraged people to report to them if they suffer a cyber-attack, partly so that they have a very clear picture of what's happening out there. But also, because they do have resources who can assist and help point you in the right direction. So, we commonly get questions, "Well, do we have to call the police? Or do we have to call this regulator? Do we have to call our insurance company?" And that's something that they can help you through on the sort of regulatory and enforcement side.

Alex Hutchens:

I mentioned insurance. You should hopefully also have cybersecurity insurance, which may be able to help respond to the problem and rebuild databases or defray some of the costs of dealing with it. And if you do have that, you should quite quickly call your insurer, because they'll be able to help and will themselves have some processes in place for dealing with things, and will ask questions that will guide your response to it.

Alex Hutchens:

And so, they're kind of the practical things you can do. Of course, we quite often get called in. We're an external law firm, and there are regulatory responses that need to be considered if you have a data breach or a cyber incident that affects certain types of information. And so, those regimes involve notification between 72 hours and sort of more like 30 days. So, you need to act quickly. And so, you need to find out quite quickly if those things apply to you. So, calling in some sort of regulatory expert will be of assistance as well.

Ainslie Cunningham:

Absolutely. So, how do you find the dealings with ... Like, you've mentioned regulatory providers, presumably the Privacy Commissioner and things like that. How do you find the dealings in that space? And managing the complexities of ... Well, obviously there'd be varying levels of degree of cyber-attack and what the sensitivity of that data looks like and the volume of it.

Alex Hutchens:

Yeah, look, absolutely. Every cyber-attack is a bit different and that's because every organisation is different. And look, the process from a privacy perspective, you mentioned the Australian Information Commissioner, the OAIC. They have a website set up for people to notify data breaches

when they occur. And under the privacy regime, mandatory data breach notification came in in early 2018, in February 2018. That basically requires you to assess whether there has been an eligible data breach, and there's a two limb test. Basically, have you lost information? Has there been unauthorised loss of ... Sorry, unauthorised access to or disclosure of, i.e., loss of information? Or have you lost information in circumstances where that unauthorised access or disclosure could then be likely?

Alex Hutchens:

If that has happened, so the physical thing has happened, then is there a likelihood of serious harm? And so, then you have to assess, once you know you've got a breach, you have to assess, well, is serious harm likely to follow for individuals? And so, that then becomes a quite complex, frankly, assessment of what information you hold, what might have been compromised, and what could be the consequences of that compromise? And that can be very different for different organisations. So, obviously if you store a lot of credit card details, bank account details, a lot of identification details, drivers licenses or something, if those things are compromised, then there's a very high risk of serious harm. It almost goes without saying, because they are so valuable from a financial fraud perspective, from an identity fraud perspective.

Alex Hutchens:

Sometimes there are some more difficult judgements to make when it's perhaps just contact details, like name, email address, address. But sometimes these which perhaps don't appear to be quite so serious on their face, can be really serious. So, the telcos and social services organisations are really alive to the issue of people who might have an AVO in place or might be in protection from an abusive relationship. And so, if their location relates very directly to physical safety, and if that information were disclosed in the wrong way or the wrong forum, then that could immediately result to a very real threat to someone's physical safety. And so, it's not a simple matter of saying, "Well, that's just a mailing address, that could never result in harm." Depending on the circumstances, it could very easily lead to very serious harm. And so, that kind of assessment is difficult to make, but is exactly the sort of thing that you need to make in order to be able to notify that.

Alex Hutchens:

But apart from those internal decisions and machinations, in terms of actually how do you notify and are they easy to deal with? The OAIC has a very good website set up. It's a web portal, where you can notify them. And it takes you through every single one of the elements that you need to complete in order to make a proper notification. And so, the process itself is very smooth when you actually get to it. And I have to say, from my own personal experience, the dealings are very professional. There is a very clear understanding that data protection, privacy breaches can happen, despite the best of intentions and despite great systems and really high levels of education and compliance. And so, it's about ... It's not a punitive exercise, if I can put it that way.

Ainslie Cunningham:

Yeah. So, you mentioned where it might just be an email address or an address. And who would make that assessment, say if that is actually compromised, somebody's physical safety in terms of, say, witness protection or a domestic violence situation? Would it be the individual whose information has been compromised to actually determine that element of threat? Because say if you're an organisation that might not be aware of that for that individual, so you would have no visibility, no understanding. How would you then know that that's become an actual physical threat?

Alex Hutchens:

Look, I guess that's one of the potential flaws of the system. You only have to notify individuals if you've made the assessment that serious harm is likely to result from the data breach. And so, it might be that you're not aware, and so make the wrong decision, or are aware and just make the wrong decision, and as a result, don't notify. And the individual is, as a result, never aware of the breach, never aware of the potential threat. So yeah, it's not interactive with the individuals in that way. The decision-making process is internal. And then, once you've decided whether or not you have to notify it, whether you have an eligible data breach, then you move forward and you tell the

regulator and tell affected individuals. But yeah, it's very possible that you are making decisions without full information.

Alex Hutchens:

In fact, it's almost inevitable you're making decisions without full information. And that's why many organisations are rightly taking quite a cautious approach to this, you know? There is no threshold, bright line test, what is serious harm and what is not? So, there is a judgment call involved. But because of that kind of risk, and because of the reputational risk that flows from perhaps not notifying, but it coming out later on, a lot of organisations are taking that conservative approach and saying, "We want to notify." And to be honest, there's a shift, I think, in many organisations' thinking. And they recognise that being up front and honest about this can actually be reputationally enhancing. Everyone understands that things can go wrong, they do go wrong. But it's actually how you respond that shows the nature of the organisation that you are. And so, yeah. I think that cautious approach that I've mentioned is a good one. There is, I think, two examples, probably, if we've got the time?

Ainslie Cunningham:

Yes, absolutely.

Alex Hutchens:

The Red Cross suffered a data breach famously a handful of years ago now. A white hat hacker actually found some records published online insecurely and let them know. And they were very open about their response. I mean, partly because of the sensitivity of the records they hold. But it was widely seen as a really ideal response and something that reinforced the seriousness with which they treat personal information.

Alex Hutchens:

There was another very famous Australian online company. They were the sort of darling of the startup world, and I won't mention them by name. But they were probably an example of a company who tried to hide away a data breach in a sort of press release that was really about something else. And it was called out. Someone noticed it. And it very quickly became the cause of outrage online. And they ultimately ended up with a notification that was complete and told people exactly what had happened and what they'd done to fix it. Actually, ended up being a really great response, it nailed everything really well. But it was tarnished by the fact that that first go out to the market was trying to just kind of hide it away a little bit, or that was the impression that came through from the way it was notified to the public. And so, yeah, it can really make a difference to your corporate standing, how you approach something like that. And there are real benefits in notifying and being open about what you've done to respond to the problem.

Ainslie Cunningham:

And what about organisations that have faced multiple attacks, like Toll or someone like that, where it just keeps being a repeat offense? Is it because they're not fixing the vulnerabilities? Or they're not doing enough of a debrief after an attack? Or they are strengthening the systems, and because they've become a target, they're just ... hackers are trying to expose further vulnerabilities? What are you seeing in that space?

Alex Hutchens:

Yeah. I mean, Toll ... You just have to feel sorry for Toll in many respects.

Ainslie Cunningham:

Absolutely.

Alex Hutchens:

It's a kind of horror scenario, having two major incidents in the space of a few months. I think it's no reflection on them necessarily at all. They have very sophisticated systems. But there are so many different threat vectors, and so many different activists out there. Activists, by which I mean sort of

cyber attackers out there. It's impossible to completely protect against all of the threats. And so, even if you do have very robust systems and very good training in place and you update regularly and you patch all of the software and you do all of the right things, with an organisation like that, that has such a huge spread around the country, regionally, around the world, and such complex systems, it's impossible to choke off everything. And so, there will just be vulnerabilities somewhere, it's inevitable, which is why we always talk about matter of if, not when.

Alex Hutchens:

And certainly, the regulators, going back to the OAIC, it's possible that you can suffer a data breach without having done anything wrong. From a privacy perspective, your obligation is to take reasonable steps to implement security measures, to protect against unauthorised access and use and disclosure of information. And you can do that. But it still doesn't mean that you are impenetrable from a cybersecurity perspective. And so, it is possible that you have a data breach, and you have to report it, but ultimately you haven't done anything wrong because you've done as much as you can. But it's not possible to be 100% secure 100% of the time, particularly because it evolves so quickly.

Alex Hutchens:

So, yeah. Look, to your point, there will be incidences, I think increasingly, of large organisations that have more than one breach or notify more than one breach. And that is just because of their complexity. And also, I think, because of just the sheer number of attackers out there trying to interfere with systems. And it might be because they are a specific target, or just because generally people are trying to attack large corporates. You can buy on the dark web, everyone talks about the dark web and you can get anything on there. But seriously, one of the very common commodities you can buy is sort of cyber-attacks as a service. You can buy denial of service attacks, and you can buy all of the hacking tools. You can buy them to use yourself, or you can pay people to deploy them on your behalf.

Alex Hutchens:

And one of the big four consulting firms does an annual report. And it sort of talks about the marketplace and there are service levels. And people have feedback, and it's a very service-oriented market. It's a very competitive market. And it just goes to show you how cyber threats have been commoditised and used by organised crime and used by people who just want to … mischief makers, as it were. So, it's, I think, that's the problem. It's now just an ever-present threat.

Ainslie Cunningham:

And they probably want the notoriety too. The bigger the name, the bigger reputation they build for themself, really, probably.

Alex Hutchens:

That's absolutely right. In chat rooms and forums, there is a lot of reputation building going on around which code you've written and what you were responsible for.

Deb Anderson:

So, are you finding that training of employees is being effective, those companies that are doing training? Or is it reactionary, rather than proactive?

Alex Hutchens:

So, look, yes and no to both of those questions. Training can be really effective. And I think that particularly around how to respond to your own personal domain, so that's emails with hyperlinks in them and SMS's that appear to be asking for information and login or contact details, that's very effective. And you can buy tools now that you kind of roll them out in your organisation and they do mock attacks, and they see how many staff respond to them. And they have click through rates. And then they provide a report, and you can kind of see what the level of compliance is.

Alex Hutchens:

Again, there's the human element. So, I've heard of training sessions in very large corporates, very comprehensive. But then, if you put a USB out that's got some ... If it says, "Redundancies 2020 on it," or something like that, the human factor means that someone will definitely pick up that USB and definitely be interested in what's on there. And so, that sort of training, training people that no matter what the USB looks like, you shouldn't be putting it into your computer, for instance, as one example. You've still got to overcome that human element. So, the training needs to be really effective to overcome that curiosity.

Alex Hutchens:

But too often, I have to say, a lot of large organisations do do very sophisticated training like that, and on a regular basis, every 12 months as part of your ongoing training, just like appropriate workplace behaviour or something like that, and just roll it out every 12 months and update it. Again, easier in larger organisations, bigger budgets, people can spend more time devoted to doing that sort of thing. Smaller organisations, I do see it tends to be more reactive. And that's just a function of everything that small businesses are having to deal with at once. And that sort of more sophisticated proactive training is not something that time permits and money permits amongst everything else always. So, I see a real mixture out there.

Ainslie Cunningham:

All right. Well, thank you so much, Alex. And I think that's about all we have time for today. But before we wrap up, is there any sort of top tips that you want to leave our listeners with today?

Alex Hutchens:

Yeah, look, we've just been talking about training. And I really do think having an increased level of staff awareness, from the CEO, who are quite often the worst cybersecurity vulnerabilities in an organisation, right through to the bottom, having that training and awareness is really important. I would say put some time into understanding what your cybersecurity posture looks like. So, what is your perimeter? What devices do you have? What systems do you have? And how might you harden that perimeter is really important. And then, I would say finally, be ready to respond. So, be prepared for the fact that this is really a matter of if and not when. But if you are prepared, it can be as painless as it can possibly be, and you can get back to business as quickly as you possibly can. And that's ultimately got to be the aim here.

Deb Anderson:

Great tips. Thank you, Alex.

Ainslie Cunningham:

Yeah, absolutely. Go and get your data breach response plan today.

Alex Hutchens:

Yeah, that's right.

Ainslie Cunningham:

All right. Well, thank you, Alex. And thank you to all our listeners. And join us next time for another episode of YS Up.

Outro:

That's all for today. Until next time, happy podcasting. And remember if you're enjoying the show, check out our other episodes and all things governance at www.3ysowls.com.au.