YS UP GOVERNANCE AND BOARDS PODCAST

Episode 11 - Cyber Part 1 - Managing Cybersecurity Risk with Shannon Sedgwick, Ankura

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.

Ainslie Cunningham:

Welcome to another episode of YS Up. Today, we're joined by Shannon Sedgwick, senior managing director of Ankura, specialising in strategy, cybersecurity, and governance, risk, and compliance. Shannon Sedgwick is a senior managing director at Ankura located in the Sydney office. Shannon has experience in providing future focus leadership to government and enterprise executives and boards to maximise the benefits of implementing new technologies, align that implementation with their strategic intent, and future-proof their organisations against cyber threats. After over a decade of working globally, consulting on technology, cybersecurity, and governance, risk, and compliance, Shannon has unique and unparalleled insight into what makes an organisation profitable and resilient.

Ainslie Cunningham:

Shannon has landed coverage in print and broadcast outlets around the world, including The Today Show, 7 News, Sky News, ITV, KBPS, ABC, 60 Minutes, 2GB, and Sunday Night. His articles have been featured in the Asia Pacific Security Magazine, Australian Financial Review, The Australian, CSO, News.com.au, and university journals. Shannon engages with executives in boards, in both government and private industry, and developed solutions to incorporate cyber risk into their overall business strategy.

Ainslie Cunningham:

His focus is on strategic cybersecurity, helping clients make risk reduction and compliance objectives and advising on the implementation of new and evolving technologies by ensuring they are secure, fit for purpose, scalable, and continually driving efficiencies in the target organisation. As a non-executive director on various boards, Shannon has a passion for initiatives that tackle issues affecting the disabled, indigenous, and veteran communities. Wow. Welcome, Shannon. How are you today?

Shannon Sedgwick:

Oh, wow. Yeah, I'm good. How are you? I'm sorry you had to read all that bio. I'm going to have to do something about that.

Deb Anderson

That's a lot of acronyms.

Ainslie Cunningham:

Honestly, it's very impressive, Shannon. So, welcome to the show today. So, tell us a little bit about Shannon Sedgwick and Ankura.

Shannon Sedgwick:

Oh, okay. Well, no, my background going way back is ex-military. After I left the military, I started my own risk management firm in San Diego in the US and had quite a bit of success there and opened up offices in Sydney and Singapore. I was bought out of that business, so I exited that successfully a few years back, and then I went and joined a big four consultancy to lead their cyber risk business in federal government and build out that business and had a great time there. And then, since then, I've joined Ankura as a senior managing director leading their cybersecurity practice nationally.

Shannon Sedgwick:

And like my bio said, we focus on strategic level cybersecurity, which is cybersecurity, which is aligned with the organisation's overall business strategy. So, we do work like mergers and acquisitions, due diligence, or cybersecurity and technology cost optimization, which is selling quite well right now with all the organisations trying to reduce costs, but to do it in a way that helps them still meet regulatory compliance and risk management standards is difficult. So, a lot of companies are enlisting our help with that right now.

Shannon Sedgwick:

And we also have another arm with the practice as well, which is going very strongly, which is our digital forensics and incident response. Yeah, that's really interesting work, and my colleagues are heavily engaged in that right now, particularly off the back of increased malicious activity, which obviously everybody heard about when the PM mentioned it on Friday to the press conference.

Ainslie Cunningham:

Yeah. So, tell us a little bit about that, Shannon, from your perspective. There seems to be a hyper sensationalism in the media as per normal?

Shannon Sedgwick:

Yeah, shock, horror. Media sensationalising things. The PM's announcement was something that we've been aware of in the industry for quite some time, particularly since the economic downturn and the lock down with COVID, the mass transition to working from home, so there's been a lot of adoption of new technology and new software. And Shadow IT's a massive problem, particularly when working from home, because IT and security teams don't have the oversight over what their employees or the staff members in the company are doing anymore. And cyber criminals and malicious actors have taken advantage of that increased attack surface or that availability of vulnerable users and technology, and that malicious activity has increased dramatically.

Shannon Sedgwick:

So, the PM's announcement, I think, wasn't anything new to us, but it may have been to Severy day members of the public and leaders of corporate entities, I think it was a wakeup call for a lot of them. And I believe anytime the government is emphasising the importance of cybersecurity is great. The more they do it, the better. And it sounds like there's going to be some added investment from both

government and private industry and some new standards being suggested for private industry so that we can increase our overall cybersecurity maturity as a nation, and I think that's brilliant.

Ainslie Cunningham:

Yeah, absolutely. What an opportunity right now to highlight this issue. I've been talking to a few people recently, and obviously you're the first part in our cybersecurity series, which will be a three-part series. So, we'll be touching on different things around the practicalities of a data breach or an incident response and the communication side of that. But from your side, being a technical specialist in your area, at least it's an opportunity to highlight these issues when the worldwide web is not exactly that old compared to other risk management traditional frameworks, in terms of managing financials and managing strategy and things like that. The digital world is really not that old. I mean, I remember growing up without internet or computers or any of those things, so yeah, at least it's bringing that opportunity to you guys and helping you, I guess, highlight the issue to new potential clients.

Shannon Sedgwick:

Well, yeah, exactly. And you only have to look at, say, specific Board Directors and governance 10 years ago, data risk or cybersecurity wasn't on anybody's radar at a Board level or a governance level. And you only had to look at, even going back a couple of years, Board Director vacancies, the role descriptions would be finance, accounting, legal frameworks, governance, very much geared towards previous serving accountants and lawyers. Nowadays, they're looking for people with that technology experience and around technology transformation and data risk and cybersecurity risk, and more and more, as we communicate these issues, they're realising it's not... Cybersecurity used to be just delegated to the IT team. "Oh, it's an IT issue."

Shannon Sedgwick:

But they're realising now it's a business-wide issue. It needs to be a strategy that's developed and driven down from the top, from the Board and the executive level, to gain buy-in from the rest of the organisation. And the more that we can communicate that cybersecurity isn't just a cost, it's not a cost centre to just bury away money and not see any return. If you conduct your cybersecurity efforts in a way that aligns with your business strategy, it's not just a cost. You can actually increase profitability and increase your resilience and increase, actually, customer trust and goodwill if you go about it the right way. And that's something that needs to be communicated to all businesses and government, is to see cybersecurity for what it is, it's no longer a want, it's a need, it's a must have.

Ainslie Cunningham:

Yeah, absolutely.

Deb Anderson:

I think in The Australian, on the weekend, Shannon, there was an article, and it said a lot of the attacks have been spear phishing and ransomware attacks. If you're a small business, what sort of mitigating factors can you put into place when you don't have big budgets?

Shannon Sedgwick:

Yeah, sure. And that's a problem, isn't it? Is you've got to think about it in a way nobody can protect everything. There's banks in the US that have an actual limitless budget for cybersecurity. They spend hundreds of millions on it every year, and even they can't protect everything. So, what hope does a cafe have or a small physiotherapy business? And what it's about is identifying what operations and what data assets and systems are critical for the continued operation and the success of the business? You look at what IT systems underpin that, and then you apply the

appropriate security controls to those systems. But a good place to start, as you said, spear phishing, which is typically down to human error, clicking on a link that they shouldn't or opening an attachment or an email that they shouldn't because they didn't identify the warning signs in the structure of that email or the sender of that email. That's often the most attributable cause for data breaches or cyber incidents occurring successfully.

Shannon Sedgwick:

So, first steps to consider as a small business would be cost effective options, so multifactor authentication. Often, that doesn't cost anything to switch on. You can do it on Facebook, on Instagram, on dating apps. Multifactor authentication, the functionality is in most newer software and applications. Then patching, making sure that your software and your operating system is up to date. And then you user training and awareness. You can get user training and awareness for $40 a year per person. It's incredibly cheap these days, or even for free.

Shannon Sedgwick:

And then, also, daily backups. It doesn't cost you anything to back up your information each day. You might have to pay a little bit more to, say, iCloud or G Drive to be able to... Google Drive, to be able to store a bit more data, but in the end, it's worth it. And all of those options, you can get them almost for free or for very low investment, and it will protect you from the majority of the cyber risks that you will face. So, to say that there's not enough budget for SMEs to be able to protect themselves adequately, I think is not a valid excuse.

Ainslie Cunningham:

Yeah, absolutely. So, in terms of actually going through a cybersecurity incident or a data breach, what are the first things that you think a business needs to do to respond? Do they call somebody with your expertise to come out and do a third-party review? Or how does it work?

Shannon Sedgwick:

Well, when an incident occurs, the first thing that a provider should do is obviously have access to the contact details of, say, a company like ours and also the relevant government agencies. So, contacting the Australian Cyber Security Centre immediately, because they can often provide immediate response and assistance without having to pay for it. Particularly those with a very low budget, the ACSC has some great assets there that they can provide help to smaller SMEs. What usually comes next is in the incident response procedures. Usually you'd hope that a business has an IRP, or an incident response plan, and they'll be able to follow those steps. When there's not an IRP, this is when it makes it very difficult and the time to respond and the time to both recover get drawn out and it costs them more every day that the business operations are down.

Shannon Sedgwick:

Hopefully, the attack wasn't ransomware, where they've turned your entire data sets and your computers into unusable bricks. But more and more, this is a favourable attack by malicious actors, and you see ransomware being used quite heavily. You only have to look at the Toll cyber-attack to see the damage that it can cause, and unfortunately, they got hit twice, which is really terrible for them. But the initial response is about minimising the damage done to the business by segmenting that particular part of the network or the systems that have been affected, and in some cases, you'll have to transition to manual work processes to be able to keep your operations going. And then calling in the experts to conduct incident response to help you guide through it to be able to restore your systems from backups, which you hopefully have because you followed my advice about having daily backups. You restore from backups and plug the gaps, plug that vulnerability where the attack originally originated, and then set about recovering and getting back to BAU.

Shannon Sedgwick:

And then after that comes digital forensics, where you look at the attack that happened, who was the user who, say, clicked on the link or opened up the email attachment? Where did that email come from? Seeking to attribute that attack to a certain malicious actor or who did it, which is extremely difficult, but it's about looking at what they gained access to and how to prevent that data that was accessed being let out into the wild, so to speak. Additionally, what's incredibly important is during that time is communication, communication with your stakeholders and communication with the data owners, which is, if you hold the personal identifiable information of both your employees or, say, your customers, you need to inform them immediately that you've suffered a data breach and that their data may have been accessed or compromised and this is what you're doing to fix it. Delaying those types of announcements only causes additional reputational damage, and oftentimes, that reputational damage, if handled poorly, can far exceed any type of financial damage or operational downtime damage that can occur due to that data breach.

Ainslie Cunningham:

Yeah, absolutely.

Shannon Sedgwick:

You only have to look at the example-

Ainslie Cunningham:

You see that over and over, don't you?

Shannon Sedgwick:

Yeah. You only have to look at examples like Yahoo when they were being acquired by a large telecommunications firm in the US and they got found out that years beforehand they'd suffer a data breach of hundreds of millions of their users and didn't tell anybody about it. And I think they had hundreds of millions wiped off their market capitalisation mid acquisition, which just shows you the damage that can occur to your reputation and goodwill. And it's hard to enumerate that damage because you don't know what new clients were going to come your way and now are no longer going to because they can't trust you. It can be incredibly damaging. But in the same turn, if you handle it well, you can actually gain more customers and gain more trust because of it.

Shannon Sedgwick:

A good example of that is the Australia's Red Cross. They suffered a data breach, not due to a malicious actor, but due to a third party error, where they published the entire list of their donors to a publicly facing webpage, including their health and address personal information. And they handled it exceedingly well. They involved the Australian Cyber Security Centre or the Computer Emergency Response team, and they helped them respond to that incident. And they were extremely clear and very forthcoming and rapid in their communication to those who've been affected. And it actually increased the amount of donors that they had afterwards because they'd been so transparent.

Ainslie Cunningham:

Yeah, definitely.

Deb Anderson:

So, with those attacks that you've seen where they've had cyber insurance in place, how effective are those policies?

Shannon Sedgwick:

So, I think cybersecurity insurance is an excellent thing for the industry, but it's not a panacea. It's not a silver bullet that is going to cure all our cyber ills. A lot of people take the view that because cybersecurity risks are unavoidable, we'll just transfer all of our risks via insurance. And you can't transfer all of your risk. It's impossible. You can't transfer it to a third party. You have to own some of it. And additionally, when you do suffer a data breach and it's shown to have that you haven't got any cybersecurity controls in place or you haven't paid adequate attention to that issue, it may actually void your insurance, or you're forced to pay extremely high premiums.

Shannon Sedgwick:

Cybersecurity insurance can be beneficial. You just have to ensure that you get a policy that is fit for purpose for your organisation and that it covers what you need it to cover so you're not paying too much for it, and also, so you can be sure that your losses will be covered should a data breach occur. And oftentimes, insurers, and cyber insurers in Australia are typically quite good, they have partnerships with organisations such as ours to come in in the event of an incident on their behalf and actually conduct that digital forensics and incident response services. And that's part of the work we do. Most of our work comes from insurers.

Ainslie Cunningham:

So, with, say, an e-commerce site, for instance, Shannon, where there are additional requirements for PCS DSS... Oh, sorry, PCI DSS, compliance with the banks, etc, around collection of credit card information and encryption of that information and de-identifying, what are the sorts of things that, with a lot of changing strategic direction and businesses transitioning to online and potentially an e-commerce site, what would you recommend in terms of those sorts of things to protect, now that you mention?

Shannon Sedgwick:

Yeah, sure. So, PCI DSS, it's not a standard when you're compliant with it that equals security, and compliance with any standard doesn't equal security. You have to take a organisation specific, risk-based approach. Again, starting in the e-commerce site, you ask yourself that question, what is most important for the continued success and operation of this business? Well, it would be the protection of that financial data that you store, those credit card details of your customers, and also the continued operation of that web page and its functionality. So, it'd be about having, to stop password injection attacks, having as simple as the captcha tools that you type in your password or you type in the information into a form and it asks you to, say, click on all the pictures that have a car inside it, or what's two plus three and then you answer it. These are questions that a bot or malicious software couldn't actually answer, so it helps provide that additional layer of security.

Shannon Sedgwick:

Additionally, having bare basics, such as a site security certificate. That doesn't mean it's a safe site, contrary to popular belief, but it does add a level of assurance. It's about defence in depth, having multiple controls in place to protect both your business and the privacy of the data owners, whose data you store. But PCI DSS, it's a good standard to have, but it is self-assessed. You can get an outsider in to ensure that you're compliant with it, but it is self-assessed, it helps you tick those boxes. But then again, a tick the box approach isn't appropriate for organisations to mitigate cybersecurity risks. There needs to be, like I said, that risk-based approach.

Ainslie Cunningham:

So, you're finding, you've mentioned, that a lot of attacks, some of the mitigations that you've just mentioned now around bots not being able to crawl that information or ransomware software, do you find that malicious attacks do come from automated software?

Shannon Sedgwick:

Many do. It's part of the tool set that a cyber attacker will use. They use automated code, automated software, to be able to attack different businesses and individuals until they find a vulnerability, and then, oftentimes, they'll use manual tactics to be able to gain further access into those systems and to be able to move laterally because, obviously, software isn't too proficient at thinking laterally and thinking like a human and bypassing the human element of your protection. So, you'll often find with more advanced spear phishing, it hasn't been automated, it's been a human behind that who's researched the company, they've done their intelligence gathering, they know who the CEO of the business is, and they can make email sound like it's coming from him to process invoices that are fake or to gain access to key individuals within the organisation with scam emails that look legitimate. There's oftentimes quite a bit of intelligence that goes into it.

Shannon Sedgwick:

Previously, attackers, particularly nation states, used to use more of a spray and pray approach where they used automated software. Now we're finding it's more specific and targeted and they've done their research, which makes it even more dangerous. And they usually target C-suite individuals within the organisation who are quite time poor, and there's only usually an EA as the gateway into their emails. And if they haven't done their cybersecurity awareness training or it's one of a myriad of emails they have to go through each day, mistakes can be easily made.

Ainslie Cunningham:

So, in terms of Department of Defence strategies and the NIST strategies and things like that, if an organisation, say, of a larger size implements all of those recommendations and tries to mitigate any risk and minimise any vulnerability for an attack, are they still exposed in some way?

Shannon Sedgwick:

Yeah, of course. Even being completely compliant at the highest levels with, like you said, with a cybersecurity standard such as NIST or ASD's Essential Eight, or if you're defence or federal government, the ISM, the Information Security Manual, aligning yourself at the highest levels with all of those standards is still not going to protect you from everything because those standards haven't been designed with your specific organisation in mind. They're a good place to start, but you need to take a risk-based approach.

Shannon Sedgwick:

Like I always say, a risk-based approach that's specific to your organisation, where you take into consideration your critical assets and the risks that are posed to those critical assets, then you use that standard to apply the appropriate levels of controls and cybersecurity maturity levels. You assess them on each of those particular business units and those assets, and then you set about applying controls that fit within your budget and that are giving you the most bang for your buck based on your risk profile.

Shannon Sedgwick:

So, there is some in depth analysis to go through at your organisation, but once you've done that, and you've got a fairly mature risk model, you can adapt the risk profile to your organisation adapt, because what's a critical asset now might not always be. And sometimes assets and operations or

acquisitions that you make or new IT systems put in place, they then become critical and you need to envelop them in your overall cybersecurity boundary.

Ainslie Cunningham:

Yeah. It's really that privacy impact assessment and information mapping.

Shannon Sedgwick:

Yeah, that's right, and working hand in hand with your security team, your IT team, data governance, ensuring that you're meeting your regulatory compliance requirements for heavily regulated industries like finance and government. There's a lot of hoops to jump through, and it's a continual effort. You can't just do it once and then expect to be secure. It's daily efforts.

Deb Anderson:

In this current cyber attack that is been experienced, I heard a report last night saying they believe it could be targeted towards research and to have a COVID vaccine. Thoughts on that?

Shannon Sedgwick:

Well, that'd be interesting. Well, certain nation states have always had a proclivity for stealing IP of other countries in order to further their own aims as a nation, so would not surprise me at all that a malicious actor has targeted IP. But particularly around COVID, we saw a huge increase in malicious actors using COVID themed emails and malicious web pages that appeared to be giving COVID-related information to the masses, and with the public thirst for knowledge regarding anything around COVID or lockdowns or people getting sick, I daresay quite a great many people fell for those scams. So, yeah, that wouldn't surprise me at all.

Deb Anderson:

Yeah, I think as you mentioned before, it's people working from home that don't have the systems in place that are properly... have been a bit vulnerable, as well.

Shannon Sedgwick:

Yeah, that's right. Yeah. And there's some people you've got to remember that have never worked from home. They often came to the office and they had a set PC that they didn't take home. It was just in the office. And then they've probably being forced to use their own device, or they've been given a new laptop from their employer, and they've had to go home and download all of the software that was necessary for them to conduct their work and they found it was difficult. So, they'll download an application or a piece of software here to make their roles easier, and the IT team or the security team have no way of controlling what they've downloaded in some cases. So, it makes it very difficult for the security teams to keep an eye on everybody with that mass transition to working from home.

Shannon Sedgwick:

Everybody that got locked down, which was most people, understood the stresses of being locked down, especially if they have a family and kids running around, and you're trying to keep an eye on cybersecurity and make sure you're not going to click on the wrong emails. And there's kids screaming and asking for things, and he's trying to sit on the kitchen table. I had friends using ironing boards as their desks in the middle of their lounge room while babysitting. You can understand why mistakes would be made.

Ainslie Cunningham:

Yeah. Challenging times, indeed. Do you have any recommendations for people working from home that they should be taking precautionary measures or any recommendations for their IT or security teams to help protect those employees and the vulnerability of the organisation?

Shannon Sedgwick:

Yeah, sure. Just constant communication about the risks that they're facing and maintaining vigilance of emails and having multifactor authentication set up across your devices and your apps, and ensuring that you know who the sender is of each of the emails and it's an email that you're expecting and you can right click on the sender to check that the email address actually matches the name. IT teams and security teams encouraging people to refresh their user security awareness training is really important.

Shannon Sedgwick:

And I think it's important as well for IT and security teams, particularly in larger businesses, is when they're implementing cybersecurity controls, a mistake that is often made is they'll implement cybersecurity controls or technical controls without any conversation or communication with the proposed end user. And what it'll do is it'll create friction in their workflows, and like all human behaviour, what do we do when we experienced friction? We look for a way to circumvent it. You only have to look at a right angle of a foot path, but there's a clear grass area that you can walk through that'll make your path faster, there's going to be a worn dirt track straight through the middle of that grass instead of walking around the concrete path. That's just human behaviour.

Shannon Sedgwick:

The same thing happens with technology and in cybersecurity, but circumvention of cybersecurity controls, obviously, that leads to data breaches. So, it's very important that cybersecurity and IT professionals work with the end users and the staff within their company to come up with cybersecurity controls that don't make their job harder and create friction in their workflows. That's really important.

Deb Anderson:

So, have you seen any statistics about an increase in cyber attacks?

Shannon Sedgwick:

Yes. Particularly since Coronavirus lockdown, there's been a huge increase even in the adoption of web pages that have Corona-related names has been... I think at one point there was about 10,000 new web pages a day, and I think that rate is still sitting at around three or 4,000 even now. And that's been the entire lockdown, so the past two or three months now. So, it's a staggering amount increase in malicious activity. There's readily available statistics, and I don't have them in front of me, but it's been a dramatic increase. And like I said, that's from a combination of things, increased working from home, the attack surface getting larger because of that, people having lax awareness of cybersecurity risks, working from home, and being distracted and that thirst knowledge.

Shannon Sedgwick:

And cybersecurity criminals... cyber criminals, sorry, always take advantage of distressing times. Even during Australia's bush fires, malicious activity increased, and there were scammers trying to tap into generous individuals donating to bushfire reliefs. They were setting up scam fundraising efforts. And whenever you see a disaster, almost always there's a corresponding increase in the malicious activity. It's of no surprise to anybody that they're not good people.

Ainslie Cunningham:

No, definitely not.

Deb Anderson:

Well, hopefully one of the many lessons we'll take out of the COVID situation will be to be conscious of increased cybersecurity.

Shannon Sedgwick:

Yes, definitely. Yep.

Ainslie Cunningham:

So, is there any top tips that you want to leave anyone with today, Shannon, before we wrap up?

Shannon Sedgwick:

Yeah, sure. Just constant awareness I think is key and constant communication with staff members and the IT and security teams, and just seeing cybersecurity as the business enabler that it can be, not just somewhere that their costs get buried and you forget about it and you hand off the problem to the IT team and the long suffering Chief Information Security Officer. It's one of the most difficult jobs you can do, and you can see why that they usually only last a couple of years in the role just from the high stress of it. But I think it's important that we're all aware that cybersecurity is everybody's responsibility, from individuals through to small Mum and Pop shops, to large corporate businesses and federal government. It's everybody's responsibility, and I think we're going the right way about it. We just need to keep ploughing ahead with those efforts.

Ainslie Cunningham:

Absolutely. Well, thank you very much for your time today, Shannon, and thank you to all of our listeners who've joined in. And join us for another episode of YS Up, and tune in for the next part of the cybersecurity series.

Deb Anderson:

Thanks, Shannon.

Shannon Sedgwick:

Thanks, guys.

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.