Take on Board Podcast – Episode 199

Transcript – Penelope Barr says there's no excuse for not taking privacy and security seriously

Helga Svendsen 0:00

Today on the Take on Board podcast, I'm speaking with Penelope Barr about privacy and security in the boardroom. Before we start that discussion, I'd like to acknowledge the traditional custodians of the land on which we record this podcast today. For me, I'm recording on the unseeded lands of the Wurundjeri people of the Kulin nation, and I pay my respects to elder's past and present, I acknowledge their continuing connection to land, waters and culture. I support the Uluru statement from the heart. And I encourage others in the Take on Board community to do the same. Now, let's hear about Penelope. Penelope, would you like to introduce yourself to the Take on Board community?

Penelope Barr 0:42

Lovely, thank you and I to support the acknowledgement of country? Thank you. So, at the moment, I'm living my best life. I'm living my 6-3-3 dream which I had in 2006. So in 2006, I was living in the UK. And I can save the notion of 6-3-3, which was that I wanted to work in paid work for six months of the year, I wanted to be able to travel and vacation for three months of the year. And I wanted to either write or create a product for three months of the year. So for the past two years, I've been doing that. And it's been great. I'm not earning quite as much money as I would like yet. But that's my vision. And so I'm really pleased that I've been able to bring that to life. So what do I do in this time that I've enabled myself to live? It's called AABCC. So I'm an advisor to startups and to corporates. I'm also an author. So I've read my first book, and I'm writing two others. I am starting a business, I consult and I also coach. So one of the businesses that I advise to is called Privay, which is a data privacy and cybersecurity startup. And that's what I'm here to talk to you about today. And you know, where this organisation sits is in terms of helping organisations and boards, practically address privacy and cybersecurity readiness, particularly in terms of systems and technologies. And I'm really about practical and pragmatic solutions. And I've worked in technology for 25 plus years, I'm not sure where all that time has gone. But you know, I really speak startup and big end of town and I've worked locally and globally. Over that time, I've had a wonderful career. I've talked about myself as a renascence woman. And that's a great term in terms of being able to sort of turn myself to most things. I'm never scared of product knowledge because I have lots and lots of transferable skills that I bring, which I'm supported by my lifetime love of learning. So I have a full kitbag of agile, lean product innovation, technology transformation and change, that I love taking around to different organisations and helping them really get to the heart of a problem. And then taking a big chunk of a challenge and then leaving people with in a better place as I leave or stay depending on, you know what I've been brought in to do. So I've been working in the business for so long that I was at the start of most of the big technical change, big digital change that's been in the industry for the last sort of 25-30 years, I started NAB's internet banking, online trading the first SMS alerts, first online applications, etc. And I've seen lots of changes over that time. You know, when we think about privacy, for example, I think about all the initial changes in terms of the first privacy policies we're writing. And I think about privacy now and data now. And it's so dramatically different. I completed the AICD course more than 20 years ago. And I've been on a couple of boards since then. And lots and lots of committees where I've used a lot of governance skills, I actually really like risk and governance. There's a lot of, you know, a lot to be brought to the fourth because of some controls that we can bring in our daily lives as well. So, you know, I managed to use a lot of what I've learned every day. I am really passionate about getting the most out of every day. So yeah, I've had a really forcing career and the moment I'm living a lot of my dreams, so it's pretty good.

Helga Svendsen 4:20

Oh my goodness, so much to delve into there. I'm loving the idea of that 6-3-3 lifestyle seed planted here. And we'll delve into the other things around tech of course in just a moment. Okay, so it's great to know some of that background and my gosh, back at the start of NAB and others in terms of the the tech changes, the first SMS messages sent out and so on amazing before we go into privacy and so on in the boardroom, as always, I just want to dig a little bit deeper about you. So Penelope, tell me about your upbringing and the lessons that you learned. You said you're a lifelong learner. So I'm guessing there's some lessons from childhood there. And you know what you've been up to and who the leading influences were on you and what you did?

Penelope Barr 5:08

Yeah, sure. So I've got four sisters, well, actually, one died, I was still to about four sisters, but five girls and six years. And we lived in a court, where there are always lots of kids. So I was almost always the oldest or one of the very few older kids. So from a very early age, I was given a role of being in charge of lots of people and being accountable for others. And that accountability included, making sure everybody was happy, everybody was involved. Everybody got a turn, everybody was entertained, and everybody was unable to realize their creative selves. My mum was a huge influence on all of us. But one of the reasons why that Renaissance woman isn't a part of me is that if we ever said we were bored, she would say go and do something. You know, I started my first business when I was about eight, and I created a 10 cent newspaper, which you could read only you couldn't have. But that was created by the neighbourhood. And we earn lots of money by enabling all of our neighbors to read our newspaper, we would put on lots of crazy concerts, which now you know, being a parent, I think, I'm so sorry, all the parents in their neighbourhood that we paid you watch all of those, the great thing about living in a court is that we all learnt to do bicycle tricks, roller skating had lots and lots of every single sport we're able to play, because we had no cars that would interrupt us. The key things that I learned there were stakeholder engagement, making sure that we really understood that everybody had to be included. So you know, do unto others as you would have done unto you, making sure that at the end of the day, everyone went home relatively happy. I kept a lifelong mental scorecard, in terms of who had won whose goal it was, who wasn't feeling great on which particular day, which parent was good to tap for which resources that we need. And also just how to draw on the skills of particular people that are needed at the at the right time. My father was also from the country. So we spend a lot of time every school holidays going down and helping out various relatives with particular requirements there had during farming seasons, and my parents were also very involved in lots of charities, and the school, etc. And so we grew up with a childhood a service. So we've all carried that into our lives. And so we're all always been involved in lots of things in terms of helping out or starting communities, etc. And so we've carried that on. So lots of lessons learned in terms of creating communities, gathering people around us knowing that we can't do anything by ourselves, and that there's lots of fun to be had, through getting people around us. So you know, I have one child. And from the beginning, we knew that we needed to create a community for her. So she was having sleepovers at very early age. And she's 12 Now, but she's still got great friends, who she started childcare with it 14 months. And I recently went out for dinner with two of my great friends as I started prep with. So that's a long, long time ago. And I still got several other friends that I went to kindergarten with, and primary school, with secondary school with university with etc. For me, there's a real joy and a real responsibility in keeping friends around you and making good friends.

Helga Svendsen 8:44

Amazing. I don't have any friends from that far back. Most of my friends that I see now are from university days rather than school. So I'm always impressed when people have got friends from that far back. And I can see Absolutely, in fact, even now as for you as an advisor, and as a consultant, and a coach, and all those sorts of things, those skills of bringing people together and knowing where the resources are keeping people happy, making sure there's some fun along the way, incredibly useful in living your best life life that you're doing right now. All right. So again, I could delve in there forever. But I really want to talk about privacy and security in the boardroom. So that pause there is me thinking what's the best question? And in fact, I think the best question is Penelope, where should we begin with this? We know it's a really big area. We know it's changed significantly over the years and increasingly changing where should we begin in thinking about privacy and security in the boardroom?

Penelope Barr 9:43

Yeah, it is a big question. You know, I think one of the key things that keeps cropping up in terms of talking to people is really around board maturity in this domain. I think the days of the sort of unwillful ignorance around this, this domain ain have really gone. So if you as an individual director, or you as a board guiding an organisation, are not up with your accountabilities and responsibilities around privacy and security, that moment has passed. And so where should you start, you should start anywhere, you know, you are accountable for making sure that you have the policies in place, that you have a privacy plan in place, and that you are testing that plan. So one of the easiest things to think about is that, you know, if we just restrict our conversation to in things that have been in the media, for example, around ransomware, or data breaches, these things can be highly emotive, if we analogize, our response to a fire drill. So we have fire drills, so that if something happens, or when something happens, we, as an organisation, and as a board, know what to do, we have a plan for it, we practice it, we make sure that we know who's in charge, we know make sure we know what to do, we make sure we know we've got communication plans in place before, during and after an event. We need to do the same with privacy and cybersecurity. So we need to make sure that we have the people in place, we need to make sure that we have an incident plan in place, we need to make sure that we've practiced the response before, I was in an organisation where we had a ransomware event I wasn't directly involved but the net impact for the organisation was that all business stopped. So it doesn't matter if you're involved in the event or not, the impact for you from a cash flow perspective, from a getting up and going to work perspective is that your work is going to be impacted, your clients are going to be impacted, everything you do is going to be impacted. Because guess what, how you made money before the event is in all likelihood going to change how you're perceived in the marketplace is going to change, how you're going to respond to events in the future is going to change. So you need to plan for these events before they happen. It's highly emotive, you don't want to be having those conversations during the event. So you need to make sure that your collective experience is planning for these events before they happen in order to get all of the directors in sync, and do the scenario planning whilst you've got cool heads. And you need to have those responses worked through before the event. So that these responses and with how you're going to deal with a ransomware event how you're going to deal with data breaches are planned as part of the incident management plan. So we know that from a public perception point of view, how organisations have responded has been a key factor in the brand reputations of the organisations. And part of it, it seems like is because the responses have been worked on the fly, they may or may not have been, I'm not close enough to know that. But that's the perception. And people are judging in a more and more harsh way. And the tolerance quite rightly, that individuals and organisations have for people getting this wrong, people have less and less tolerance for that, quite rightly, because we are handing over our data as individuals to organisations to protect and it needs to be dealt with in a respectful way. Now these decisions need to be made in relative to the organisation Iran, the decisions you need to make as a hospital, for example, are quite different to those that you would make as a social media company because of the nature of the data and the consequence of paying a ransom or not. So you know that sort of we do not pay terrorists response doesn't really work for me, because my parents, for example, were caught up in the Medibank data breach. And whilst on one hand, I can absolutely understand why at an organisation level, you don't necessarily want to encourage an industry where cyber criminals are rewarded. Absolutely. I get that. Equally. If my data were being traded, I might not necessarily want that because I've no control of where that data is going. And really what we're talking about is the data of the weakest of the weakest of us. And at some point would I become subject of blackmail or some other event in the future? I may or may not be but there's always that risk. And if you're paying ransomware what guarantee is there that that data has actually been destroyed.

Helga Svendsen 15:04

So I'm interested in that Penelope, because you're talking about, you know, what boards should do around ransomware. And quite often there is a much more black and white response than the one you're giving. So I'm wondering if you can, I mean, it's a hypothetical, obviously, and you won't have all the information. But I'm wondering if you were on the board of Medibank, when that data breach happened, talk me through what you might have done.

Penelope Barr 15:28

Yes. So I'm sure that the technology director would have been really in the spotlight. But the first thing that would have been happening for me is that I would hope that the whole board would have been seeing that this is their everybody's accountability, because the key issue that I'm trying to get across here is that privacy and cybersecurity are the accountability of everybody in the board. We've gone beyond the point where this is the kind of be the ability of one person, I would be hoping that everybody would be really facing into this. And I think part of the issue that I was observing was that I'm not sure I was a little bit lackadaisical. Choice last week, came out and said that 85% of consumers don't believe companies are doing a good job with data. I would hope that as a director, I would be really there and saying, Okay, we really need to think about this. Sometimes, what happens with data breaches or ransomware attacks is that, you know, people know that they have to replace their computer systems or their databases. But the key issue with that is that, you know, do you know that you might not know whether or not there's still a password, or something nefarious within your systems, that might be still hidden. So you would want to be bringing in some cybersecurity experts, which I'm sure that they did. But you don't always want to be relying on just that information as well. So you need to be making sure that you've got your own, you know, enough, not enough to, you know, that phrase, not enough to be dangerous, but enough that you know, enough to be able to sort of understand what you should do first, and then next. And then you do want to make decisions based on you as a board and what's good for the rest of the business. So there needs to be an understanding that this is going to impact the rest of the organisation. And how long is this going to impact the rest of the organisation. So you know, there's going to be an impact on your cash flow, there's going to be an impact on whether or not customers are going to trust you, from this point on, you're going to have to recover quickly, you're probably going to lose some customers immediately how you're going to retain the ones that you have, how you're going to get those customers lost back. They're things that are not necessarily the immediate things because you've got to recover the situation first, but they're almost day to actions. And so they're things that, you know, when I was talking before about the incident management plan, they are the things that you also need to be thinking through. So this is where the scenario planning has to move beyond just, you know, we'll have the phone numbers of the cybersecurity people that we might bring in to restore our system, you know, adopted by some backup, that's just not enough. Because these kinds of incidents have the ability to completely destroy your business.

Helga Svendsen 18:27

I was caught up in the Optus breach, not the Medibank. One, but the Optus breach. And by the end, I did not believe any of the comms I was getting from Optus. I just couldn't believe it. Because it was so often wrong. That's an excellent point. I think it's a it's a data breach. But it has financial implications. It has staff implications, it has customer implications, all of those things. So having the comms right for all of those things. I hadn't thought of that in terms of incident management rehearsals. Oh, there's probably more on that. But I'm also keen to talk about the new Privacy Act submissions as well. But just before we turn to that, anything else, we should be just thinking about that

Penelope Barr 19:09

So what can you do? Because I think that's, you know, it's really important to think that the fight is not over. It's just it's really important to, for people to be on the front foot. And this is why I make the point that it's not one person's responsibility, you know, you really need to be clear about why you're collecting any data. We know that most organisations have too much data, you really need to be identifying where the data is, and be really suspicious about any large buildups of data. And, you know, because if you don't spot that this stuff is sort of sliding out of control. You're suddenly in a position when it where if it's gone, you can't get it back. And then you have to have a conversation about whether or not you're you're potentially paying a massive amount of money to sort of get it back or not where Some work up front might have been good. I was working in our financial services institution a few years ago, when we've had to do a big purge an archive piece of work, because it was really impacting the frontline systems. So people couldn't identify the customers coming into branches or on the phone, just because the systems were so sluggish because extraneous amounts of data had been collected for years and years, which was just clogging up their systems. And so the initial response was, let's just buy more databases, it's like, well, before we do that, let's have a look at what's actually happening. So we sort of lifted up the hood, and found that, you know, it was taking between 10 and 30 minutes to identify customers, after a nine month piece of work, it got down to sort of 30 seconds to a minute to do that. But it was a big, big piece of work. But it was well worth it. We didn't have to buy any new databases. But we then knew what data we needed to collect. We had to change, you know, a lot of internal processes. But the net benefit was much heavier, internal staff, much happier customers, and much better functions, as well as much cheaper technology bill from a storage or protection or just disruption perspective, because all of the policies around a collection, storage destruction, were all much simpler. So it does take a lot of work, but it's well worth it.

Helga Svendsen 21:23

Yes. And it's a bit invisible. I think now information like in the old days, when you had archive boxes sitting in sheds, you would never go and get another shed, it would just be like, let's clean, like, what do we need and what don't we need, let's get rid of it. So digital data should be the same. You don't have to buy extra storage. But as you say, it's better for the customer, and that you're not holding their data that can then get stolen. So there's some excellent tips in there. I love the fire drill analogy and making sure it runs so that you know exactly what you're doing and that it's broad. And yeah, cleaning out your data. So I do want to turn to the Privacy Act submissions. So first up, tell us about this is the Australian Privacy Act being reviewed by the federal government, maybe talk us through what that process is and why it's important to think about.

Penelope Barr 22:18

Yes. So it's been 25 years since there's been a Privacy Act review. So take your mind back to 1998. When the internet was very sluggish, we had dial up modems, and we use floppy disks. So we use our floppy disks with my master's thesis on it for coasters for dinner parties. And we have to explain to some of our guests who are younger than us, or two kids that we have around what those things actually are. And we love making the noise of a modem, or we dial it up just to explain it. And that's when the first Privacy Act was created. So I was at NAB at the time running nab.com, the second version of that and was creating that first privacy policy along with the chief privacy officer at the time. And so that's how long it is, has been since there was a revision. So you can imagine from a technology perspective, how many changes have happened in that time, and how much there is for this Privacy Act to catch up on the submissions on a closed on 31st of March this year. It's not yet passed into law, it's likely to take a bit of time, there's no there's no timeframe, that's been suggested yet. But there's a couple of really key changes that people need to be aware of. So the first is direct, right to action. So this means that people are going to have the ability to start suing. So now it means there's not a regulated problem, it means whether or not you want Slater and Gordon to make a matzah, or few because they will. So that's a really key change, it will have immediate indirect impacts on organisations. So that's a really important change because it's going to hit people where it really hurts. And then we'll see how much money people have for making privacy and cybersecurity changes.

Helga Svendsen 24:17

I was just gonna say that they will nothing like that to focus the attention on clearing out the information that you've got, or making sure your systems are strong, interesting. Absolutely. Great thing to know and be prepared for.

Penelope Barr 24:33

Another is the types of data that are going to be collected. So there's going to be an expansion of private and sensitive information. So it's going to extend to include genomic data, find out grained location data and data related to children. So data related to children's a bit murky now. And also data related. to employees, so for example, addresses, so that's going to have a real impact. Another impact will be individuals rights for deletion and correction. So people are going to be able to ask for deletion and correction of their own information. That's, that's not in play now. And then one that's really important for the Australian economy of which 90% of businesses or small businesses is that the small business exemption that exists now is going to go away. So at the moment, we have a law that most businesses in Australia are exempt from. So that's also going to be quite impactful. So as I said, it's still at the proposal stage not signed into law yet, but if any of them by themselves happened, they would have a real impact. But if all, and it would be a completely different law.

Helga Svendsen 25:55

Loads of stuff there to think about for the organisations were on the board of and might I say, for me, as a small business owner, as well need to think about, I would hope my systems are good, but I better check on that as well, in terms of my own protection. And in fact, now that I think about even some directors, whilst they're directors of boards, they are probably their own kind of small business in some way in that kind of portfolio career as well. So I've been thinking about the information they hold as the directors of organisations and where that information is. I mean, I know, we don't know, submissions have just closed on some of these proposals. What would you expect might be the timeline for this?

Penelope Barr 26:40

Or you'd hope it would be this year? But I mean, it's been 25 years between.

Helga Svendsen 26:47

Right? So 12 months would be good. Yeah, a couple of months and 25 years? Yeah. So what would be something in 2023? That directors need to get their head around? I hadn't heard any of those things. That is excellent. Insight for me. And I might be asking some questions at my next board meeting. And even the tech committee that I'm on for one of them about some of these things that are coming up that he's fantastic. Oh Penelope so much in here. What are the key things you want people to take away from the conversation that we've had today?

Penelope Barr 27:16

I think one is that all directors have accountability across privacy and cybersecurity. You just can't get away from that. You know, I think that if something goes wrong, it's everybody has an input. I think, you know, making that incident plan and testing that without the emotion of an incident happening is a really, really smart play. But it's also required, so that, you know, what the roles are, that everybody's going to play, and that you know, what your position might be, you take the time to do that scenario planning. One thing I didn't talk about, but I think that is important is whether or not in cybersecurity and privacy is updated, and your board meetings, you know, how you're going, you know, when you talked about where would you start, you know, if you're just starting in this space, you definitely need to be, you know, starting that updating process. But even if you have started, you know, how you're going, and what what is happening in this space. And the organisation and the public's response to I didn't know or I wasn't prepared, or we didn't have enough money, or we didn't have those systems in place. Any of those excuses that we might have accepted a couple of years ago, they just don't fly anymore. So you need to have your responses in place, you need to have your systems in place, you need to look at what your organisation is doing. Or you need to have the policies in place. And you need to set your organisation's are for success in these domains. And make sure that you're managing for when these situations occur, not if.

Helga Svendsen 29:00

And is there a resource you would like to suggest or recommend for the Take on Board community?

Penelope Barr 29:06

Um, there's a little bit of self interest in this one. But from a prevention perspective, the Privay organisation has created a board checklist, which can be found on the website. And that's really a checklist just to get an understanding of where you might be from a readiness perspective. And so if you complete that, then that you'll be emailed the results and the organisation can follow up with you. So that's a good resource.

Helga Svendsen 29:32

We'll make sure there's a link to that in the show notes as well. Oh, Penelope, thank you. So many, just really practical tips in there. Like I said, I'm going to take some of them away. So thank you so much for sharing your wisdom and your insights with the Take on Board community today.

Penelope Barr 29:49

Lovely it thanks so much for having me.

Transcribed by https://otter.ai