Take on Board

Transcript – Hannah Browne

Helga Svendsen 0:00

Today on the Take On Board Podcast, I'm speaking to Hannah Browne about cybersecurity. First, let me tell you about Hannah. Hannah is on the board of Greenpeace Australia Pacific, and she's the chair of the nominations Committee, which is how I first met her a couple of years ago. She also reports into an advisory board as the managing director of Midnyte City. Hannah is a technology leader and entrepreneur and is now building her fifth tech company in Midnyte City. For 15 years, she has worked on strategic transformation initiatives with startups, scale ups and innovative enterprises, helping you build high performance teams and progressive digital first human centric organisations. Her core skills are in technology, leadership, organisational development, building high performance, culture, and influencing for change. Welcome to the Take On Board Podcast, Hannah.

Hannah Browne 0:47

Thanks Helga, it's great to be here.

Helga Svendsen 0:49

So Hannah, as always, before we get into this conversation about cybersecurity, tell me what's something from the last month or so that you're proud of?

Hannah Browne 0:58

Oh, look, as you know, being on the nominations committee with me at Greenpeace, we've been pretty busy over the last month, one of the things that has been amazing and really void my confidence coming into 2021, as we move past or hopefully through the COVID pandemic and out the other side of it, we've been looking at potentially engaging some very experienced Pacific Island folk, with the Greenpeace organisation around some strategic objectives in that area that we expect to be working on this year. And having the opportunity to connect with some incredible cultural leaders from that area of the world around how we can better impact environmental outcomes around climate change has been an absolute one of the greatest privileges of my career. And, you know, I always imagined I'd be able to make a difference. But being able to make a difference by connecting with people who are deeply experienced and very passionate about issues that I'm also passionate about and, and how we can work together to affect great outcomes in regards to those issues, has been a real honor. And, and something that I only ever imagined I could do. And and it's

been it's been a dream coming true, really, in the last month doing that work on behalf of Greenpeace. So

Helga Svendsen 2:26

I mean, that is awesome to hear on so many fronts, partly because I'm on that nominations committee with you. And it's great to hear that we've got some pretty incredible sounding candidates by the sounds of things. So that's great. And it's one of the things I love about boards is, you get to meet some of these incredible people outside your own kind of world like you're a tech person. That's why you're here with us today. And through your board role with Greenpeace that you are talking to, you know, people from various Pacific Islands about climate change, and how they might be able to make an impact at Greenpeace. That is awesome, Hannah, we're talking cyber security today, we're talking technology, but you'd need to imagine and I know this will be hard for you to imagine but need imagine that I'm perhaps know very little about technology. So speak to me, like I know nothing, which perhaps might actually be the case. But anyway,

Hannah Browne 3:19

No problem.

Helga Svendsen 3:20

So cybersecurity, it is on the, you know, it's on many a board agenda, or at least on many a board radar. And at the same time, I know it's something that really intimidates a lot of directors because they feel like they don't know enough about it. You know, much like my introduction there. It's like, Oh, I don't know enough about this. So where should we begin? What should our board members be thinking about in relation to cyber security?

Hannah Browne 3:47

Yeah, it's a great question. And I think with the government challenge, governance challenges that have emerged over the last couple of years we've gone from cybersecurity and culture being relegated to the lower order important issues for boards and executive teams to being really elevated, particularly after the financial services Royal Commission. Cybersecurity and culture are now kind of the new kids on the block that a incredibly high profile topics for boards to be considering and talking about. So that leaves us with a bit of a conundrum because the boards that I've interfaced with over the last 15 years of my career, there hasn't been a depth of technical talent and capability in the boardroom. You know, we see a lot of lawyers and a lot of accountants around the board table. And I think what we will see as we've seen in the past 10 years with the women on boards, movement from 9% of ASX boards 10 years ago to 29% now, which is fantastic, fantastic outcome for everyone involved and people like yourself who've been helping fuel that that

momentum to drive that outcome. I think over the next five to 10 years, we'll see a huge influx of technical capability into boards, as we've seen through COVID, and the move to full remote work instantly, tech underpins so much of our organisations and it did before COVID. It did before we were all working from home and using productivity tools and the Internet to remain engaged with our organisations. I think what we need to see over the next five to 10 years is a recognition at a governance and board level in Australian organisations of just how important that tech knowledge in the governance sphere is.

Helga Svendsen 5:31

I agree. There's lots of lawyers and accountants generally on boards and a range of other people as well. But it's interesting if we get I mean, we'll get into what boards need to know about that in a moment. But if they have an inverted commas technology person on their board, how did they then I mean, you're the technology person on the Greenpeace board. How do you make sure the rest of the board is also with you in the knowledge because they can't just outsource the decision making to you just like you can't outsource you can't look at the finance person and go so Treasurer Are we okay? are good. Treasurer says we're okay. So how do you bring the board along in those conversations?

Hannah Browne 6:07

Ah look, as you've taught me so many times through the podcast and that amazing book by Robyn Weatherby "Eyes Wide Open" it's all about asking the right questions. So when we're thinking about cybersecurity in our organisations, not only have we got a moral and ethical and a legal obligation to adequately protect our staff, our beneficiaries, our donors, our stakeholders, you know, we've now also got legislative requirements that around data privacy and protection that can potentially have a massive liability impact on organisations. So thinking about in Australia, we've got the notifiable data breach scheme, which dictates that you need to notify organisations like ASIC and the Australian Government, if you've had a breach of your data, you need to disclose that in a certain amount of time. But more catch all is the general data protection legislation, which is the the general data protection regulation, which is regulation out of Europe, that has considerable implications for organisations in the management and storage and management of user data and personally identifiable information.

Helga Svendsen 7:22

And my understanding is that even though that's that applies in Europe, if you've got people on your database, for example, from Europe, then it applies to you as well, indeed here in Australia, or or wherever you may be, the US, whatever.

Hannah Browne 7:33

Yeah, that's right. So you need to be aware of those things, even though the European regulations indeed. So from a liability perspective, organisations need to be asking these questions, are we managing our data appropriately? And have we taken the appropriate steps to ensure that we're protected as best as possible from a breach or cyber attack? So a cyber attack or a data breach in terms of its impact on an organisation is the first big consideration that you think he about is staff, beneficiaries and donors personally identifiable information, so anyone connected with that organisation be that customers, be they suppliers, be they donors if you're a not for profit director, internal staff protecting that, that data, having that data out in the wild can lead to potentially disastrous implications for your organisation. If you are subjected to a data breach or a cyber attack, you can expect a significant disruption to your core operations and services in order to manage and recover from this breach. Imagine you lost all of your donors personally identifiable information and credit card details one day, what sort of people redeployment internally, do you need to do what what work do you have to take people off and put them on to be able to recover from this situation and come back from that? And then, of course, that you know, the key issue for directors here and officers is the exposure of the organisation to liability as a result of this you're considering massive tarnish to the organisation's brand and reputation and we know that things can move very quickly in the technology space. Even over the last week, we've seen a huge transition of people from using the social media platform WhatsApp for texting, to more secure organisations like Signal like Telegram. Elon Musk tweeted, you know, just use Signal in response to someone complaining about WhatsApps new privacy policies. And we saw 25 million people join Telegram and 25 million join Signal in three days. So the technology landscape can shift that fast if you are subject to a breach that releases personally identifiable information, particularly payment information for anyone connected with your organisation. You may find that 50, 75, 80% of your donors, your customers, your suppliers, abandon you overnight and move to other organisations. I guess there's probably less, there's less connection to a messaging app, then there might be to your favorite charity or organisation. But the ramifications are still dire nonetheless.

Helga Svendsen 10:13

So you would expect, you know, you would hope all organisations have some sort of cyber attack plan in place, a policy and a plan, that would be what they're doing to prevent it. And then what happens if it happens? Presumably, absolutely.

Hannah Browne 10:28

This would be my advice to any director that's listening out there. At the next board meeting, you want to ask what the policies and processes are around cybersecurity in your organisation. So for the directors out there who want to be active on engaging with this issue, the key thing that we can do as directors is ask the question. So two critical questions for directors to ask at the board table? Do we have the capacity and or the capability to protect our staff, our customers, our suppliers, our beneficiaries, our donors from malicious digital attacks? Do we have that capability in place? The

second question is, are we ready to meet the increasingly stringent data privacy standards and regulations? You know, like the GDPR, like the notifiable data breach scheme, and consider the penalties for non compliance with those? I think those two questions alone could uncover an absolute treasure trove of information around how organisations consider cyber security, how they treat digital assets, how they protect the privacy of the stakeholders, all of which directors need to understand to be honoring our fiduciary duty.

Helga Svendsen 11:41

And so in that for boards to understand it, what's your recommendation around even the structures around that? Like, do you think every board should have a technology subcommittee for the better word?

Hannah Browne 11:52

Well, perhaps not a subcommittee, but at least one person who has a depth of skill and experience in the technological space to get going, you know, we need to start the conversation around this, it needs to be something that's on the risk register with the other organisational risks as part of the Risk and Audit Committee, perhaps on any board. And the organisation needs to discuss this across the board across layers of management. The best place for us to start in any organisational journey around uncovering the current state of cyber readiness is some form of vulnerability assessment. So the National Institute of Standards and Technology in the States has a great framework NIST. There's other cybersecurity frameworks out there, working with a trusted security partner to conduct a vulnerability assessment should give the board and the organisation a pretty clear indication how ready they are, what the gaps are. And whenever you're doing these kinds of assessments, it's really important to consider what good looks like there's no 100% protected when it comes to cybersecurity. It can be likened to the the analogy of using condoms. They're not 100% foolproof all the time, but they'll certainly keep you out of a fair degree of trouble. And there's a short list I'd love to share today with you if you're happy to that directors can use as a bit of a gauge that if you've got these things addressed in your organisation, then you're well on the way to having good resilience already in place. These are things like do you have a disaster recovery process in place? Do you have two factor authentication across your organisation? For anyone accessing systems with sensitive data? Do you have a policy or a procedure in place for a cyber attack? And how you would respond in the event of a cyber attack? Again, this is so important for directors fiduciary duty to be served. You need these things in place in every organisation. What insurance do you have around cybersecurity? This one's a bit more technical. But are you monitoring your network's Midnyte City is a specialist DevOps consultancy? And one of the things that we do is help people with monitoring and logging, which is assessing your tech ecosystem, and reporting back measures and metrics on the health of that at any given time. So if you're under attack from a state based actor who's trying to DDoS your organisation

Helga Svendsen 14:29

You've got to slow down on some of these technical stuff. DDoS

Hannah Browne 14:33

Denial of Service Attack, they will hammer some form of login to access your systems. Yes. And it's called a brute force attack where they try and bust in the door basically,

Helga Svendsen 14:44

Now that we know what a DDoS is go on.

Hannah Browne 14:47

The last point I would I would give to directors to ask about at the board table is is what form of ongoing training Do we have around cybersecurity for the team? One of the reasons I I'm interested in cybersecurity the social engineering aspect of it, how people get in other people's heads to get login credentials to be either held, you know, to sort of ransomware attack or the victim of some form of fraud, and phishing emails, we all get them all the time, you know, text commonly in text messages and emails, asking for private or sensitive information claiming to be from one of our big banks or a trusted telco provider, that whole aspect of the technology industry, I find absolutely fascinating. And you can't build systems or firewalls against human behavior. So ongoing training and guidance for the entire team around cyber resilience is super critical. Because if you've got someone who's got access across a broad range of your systems, and they're not protecting their password and their access credentials, effectively, your organisation could be liable for a massive data breach, these things are crucial, and they're not tools that we can implement their ways of working. When it comes to the humans in our organisations,

Helga Svendsen 16:07

Yeah, I've heard this a number of times that we're not going to prevent it, as you say, we haven't talked condoms on take on board before. But I, you know, I think it's probably a reasonable analogy. In this instance, you can't necessarily prevent it happening. You can minimize it and have in place protections so that it doesn't and training and all of those sorts of things. I know you're not on Facebook, which, you know, I admire greatly. But all those stupid surveys that go around on Facebook, asking about where you grew up, and you know what your pet's name was, it's like, Oh, you mean the answers to all of those security questions? Yes,

Hannah Browne 16:41

And asked all the time. 100%. That's exactly what they are. We're going through a very painful time in human history right now, where we've got these, you know, social media is relatively new to the human race. And I remember the early days of social media, when it was hailed as this connector right across the globe. And, and we've seen it during the Arab Spring, how those social media platforms we use to coordinate protests. And but the flip side of that is, you know, we've seen the Trump supporters on Parler in the in recent weeks using that to coordinate assaults on American democracy in the Capitol, like these are at the end of the day, all technology is just tools. And they just enable humans to do human things using new tools. So I think we've had a very painful and creaky introduction to social media. And it's one of the effects of that, that I despair over is how we share our data. We do not care seemingly, who knows what about us, we post stuff on Instagram, on Facebook, on Twitter, on LinkedIn, and all of the other ones that I don't keep up with, because I'm not in that space anymore. We just give it away for free when like, it's not important to us at all. And actually, the way AI is coming around now and growing and developing, potentially, we're setting ourselves a real rod for our backs. Yeah, as we move forward. So I think there'll be a swing back towards privacy. In my humble opinion, I think people are starting to take digital privacy a little more seriously. And the fact that we have a right to privacy online, we don't, we don't need to sign up to be spied on by the social media companies and the big tech giants and have everything every keystroke we ever enter into our computer or phone recorded so that some organisation can analyze our behavior and sell us consumer items more effectively. I think we'll see a swing away from that over the next couple of years, because I don't think it's necessarily very healthy or supports a really robust, psychologically well adjusted human race.

Helga Svendsen 18:48

So if there is a swing back to privacy, like I think, for organisations or for board members of organisations, there's two sides to that. One is that, hopefully that means the individuals that work within that organisation become more careful about their data so that it makes it a bit safer. But what should the organisation's themselves be thinking about in terms of potentially a swing back to privacy? Or, you know, for those organisations that are on LinkedIn that are on Twitter that are on Facebook that are on Instagram? What should they be thinking about?

Hannah Browne 19:19

Look, great question. When Edward Snowden revealed some years ago now that the NSA was collaborating with tech giants to covertly surveil both foreign and domestic residents of the United States and all kinds of people all across the globe. I was working at Thoughtworks. At the time, they were heavily involved in a in a global response to online data privacy. And one of the things that Thoughtworks talked a lot about at the time was be sensitive about the information that you're collecting. So as an example, every now and then I'll do yoga at a yoga studio in Northcote. Not very far from here. To do yoga at that studio, they want my first name, my surname, my phone number, my email address, whether I've got any previous injuries and a laundry list of other questions, which,

if you step back for a second and think about it, why does a yoga studio need to know that about me, for me to be able to do yoga, it's not appropriate, it's disproportionate to the services provided for organisations. And this is probably more for the management team than the directors be really conscious and cognizant about the information and data that you are collecting. Do you need that information from those customers to effectively deliver that service? Now, what I've personally seen in the last five years, which is a symptom of the environment that we are in, and the place and time in history that we are in, is this land grab for data, every organisation has seen Google and Facebook, monetize customer data, and sell advertising space, and commercialize that incredibly effectively. And so now you've got every organisation in the world scrambling to find out everything they can about everyone who interacts with their organisation, so that they can feed it into the AI machine and get in inverted commas insights out the other end, which is how can we monetize this relationship more effectively? That, to me is dangerous, it's set a precedent that's disproportionate to being able to provide the services that we need. And I think, you know, for me, I deeply respect organisations who only collect the data that they need, even just in relation to this cybersecurity event that we're running on the 29th of January, in putting together the form for collecting the information for that. I'm thinking very deliberately about what's the minimum I need from anyone who would like to listen to this workshop, this seminar, so that we can provide that service. I don't want more information than I absolutely need to provide that service. That's the paradigm shift of thinking, I guess, is not let's take as an organisation, there's this idea of let's take everything we can get. And I think that's I don't think it's appropriate. I think it's wrong, and it's dangerous. I think we need to be thinking about what we need to provide the best service and respect the rights to privacy that our customers and stakeholders have.

Helga Svendsen 22:15

All that additional data brings additional risk for organisations, because if you lose it all.

Hannah Browne 22:20

That's right, yeah. And I remember when JP Morgan's hack happened a few years ago now. And I just shook my head. And I thought, well, if JP Morgan can't get this right, with all of the resources, and the money and the capability that they would have inside those four walls, like every organisation is vulnerable to attack in some way, shape, or form. And it's not a case of if it's a case of when. So as directors, we need to be prepared. And being prepared for me goes right back to what are the decisions we make around the data that we collect in the first place?

Helga Svendsen 22:53

Yeah great point. However, I knew this would happen. We're coming to the end of the time. So what are the key points you want people to take away from the conversation that we've had today?

Hannah Browne 23:04

Look, thanks, Helga. And it's been a real pleasure to be here. For me, the questions around the directors need to ask around the board table is the critical thing here. So do we have the capacity and or the capability to protect our staff, our customers, our stakeholders, our suppliers, our beneficiaries, our donors from malicious digital attacks, and we ready to meet the data privacy standards and regulations. So the GDPR and the notifiable data breach scheme, and the penalties associated for non compliance. If every board in Australia as those two questions over the next couple of months, we could potentially prepare our whole economic landscape to be more resilient to cyber attacks. And the way technology is exponentially evolving. This problem isn't going to go away. It's always going to be an arms race, it's always going to be about protecting yourself as effectively as you can for the environment and landscape at the time. And that's going to require vigilance and ongoing investment.

Helga Svendsen 24:07

Well, that's very handy for me, Hannah. I'm just about to join the finance and IT committee of one of my boards, and I can turn up with a couple of questions at the next committee meeting to ask about that. Perfect, great advice for me. So can you recommend a resource for the Take on Board community?

Hannah Browne 24:24

I look, Midnyte City's running a cyber resilience seminar for it is specifically for nonprofit directors. But I suggest for organisations and boards that don't have a depth of technical capability on the board. There will be learnings there for every director, running that on the 29th of January at 12.30pm. And I can give you a link for the show notes for people to anyone who's interested to register.

Helga Svendsen 24:49

That would be fantastic and registering of course with only the minimum amount of information required - no phishing going on here. Oh, thank you, Hannah. That has been so useful as I say I know technology and cybersecurity is on the radar for all well, hopefully every organisation, and I know that it is something that well intimidates the hell out of many directors. So I think that's provided such a fabulous summary for directors to think about at the board table and to look clever, which is fantastic. So thank you so much for coming and sharing your wisdom with the take on board community today.

Hannah Browne 25:24

Thanks for having me Helga.