Take on Board

Transcript – Insights from the Take on Board Breakfast: Cyber security with Hannah Browne - Part 1

Helga Svendsen 0:00

Hi folks and welcome, we will officially kick off to the first take on board event for 2021. So thank you all for being here and I know people are continuing to join as we go. I would like to start by acknowledging the traditional owners of the land on which we variously meet. For me, I'm in Thornbury in Melbourne. So that is the Wurundjeri people of the Kulin Nation. I know different people are in different parts of Melbourne and even beyond. So paying respects to traditional owners, whoever they may be, wherever you are, and to elder's past, present and emerging. So today, we will be hearing from the fabulous Hannah Browne, who for me is there in the she's waving, so you know who she is about cyber security. And we know, this is such an important issue, not only an important issue, but also one that not everyone really understands. So Hannah is going to demystify and give us all sorts of practical wonderful tips that we can take back to our boardrooms or to our workplaces, whatever that might be.

Firstly, I know Hannah through she and I are both what we started on the Greenpeace nominations committee together I think three years ago is when we started our time together there. And Hannah is now on the board which is magnificent. And I should say, a alumni of the Board KickStarter program, and also now on the Board Accelerator program. Now that she's on the Greenpeace board, which is just fantastic. So she's now Chair of the nominations committee. She and I are both on what's called the General Assembly, which is kind of the membership of Greenpeace and you are invited to join committees. And then they are chaired by the board. So she has switched from being a participant to the chair of it as a board member. Enough about that board stuff. Let me tell you about her tech experience. So she's a technology leader and entrepreneur now building her fifth tech company, Midnyte City. For 15 years, Hannah has worked on strategic transformation initiatives with startups, scale ups and innovation, innovative enterprises, helping to build high performance teams and progressive digital first human centric organizations and don't we need more of them? Her core skills are in technology, leadership, organizational development, building high performance, culture, and influencing for change. Hannah is on the board of Greenpeace, as I said, and chair now of the nominations committee. She also reports into an advisory board as the managing director of Midnyte City. So Hannah is going to take us through how to prepare or prevent a cyber attack, how to protect your privacy, and no doubt all sorts of other awesome things. Alrighty, Hannah, over to you.

Hannah Browne 2:45

Thanks so much Helga. And I'm super excited to be here particularly off the back of our all of the energy and excitement around our cause that happened yesterday. I was also at the market yesterday, Helga called me at about 630 last night, I usually call to check in on the on the speakers for the next day. But I got caught up in the March For Justice. And I was like, oh, like, how great is that. So I'm going to talk a little bit about cyber security today. Thank you for the great introduction Helga. And I'd also like to acknowledge the traditional owners of the land on which I gather which in in Alphington in Melbourne is the Wurundjeri Woi Wurrung, we're on people of the Eastern Kulin Nations and pay my respects to the elders past, the leaders here in the present and the future leaders. As Helga said, I'm on the Greenpeace board, which has been very exciting. I've been there for about six months now and already learned a stack which is great. I also chair the nominations Committee, which I think is a really crucial committee for any board. It's really the future of the organization and the governance of the organization. And my company, Midnyte City is a technology consultancy. The fifth one that I've built, we focus on DevOps. DevOps is a way of delivering software more effectively. So it helps optimize the outcomes and outputs of your technology team. And a lot of the work that we do is about security, and agility and resilience in the architecture of the technology that underpins everything that we do. Essentially, here we are meeting today, we're all staring in laptop screens using the internet and telephone cables to be connected. So that leads really nicely into my first point. So I'm going to run through some key themes today. Let me just run run you through what they are. So we're going to talk a little bit about the anatomy of an attack. So I'm going to talk a little bit about the NotPetya attack and the impact that that had on Maersk . But that attack cost Maersk $300 million. And it took down the entire organization. We're talking 80,000 employees 574 offices in 130 companies and shut down their entire operations for over a week and never mind on all of the goods that were stuck in container ships and dock yards and on ships, and that got lost in inventory, but that's going to give us a bit of a sense of how bad things can go when cyber security goes wrong. Next, I want to talk a little bit about, and we'll give you a cheat sheet as to how to start as a director with our fiduciary duties, how we can make sure that our organization is as resilient, as is sensible against cyber cyber attacks. So my first point, though, and I think this is the most important one, if there's nothing else you take away from this today, and I'm happy to be wrong about this, too, I might be very wrong in this point, but I don't think I am. I look at governance, and I look at you know, if I zoom out in the last 10 years, we increased and you know, thanks to amazing humans like Helga, and people like her, we've increased the representation of women on ASX 300 boards by something like 20%, it went from about 9%, up to about 29% in the last decade. Now I believe that the next decade will see a similar trend. But it will be technology people moving on to boards. And my first point is, if your board has nobody with a background in tech, that is a skill gap that you need to address immediately. I shake my head in wonder at organizations who run multi million dollar budgets and organizations who are spread right across the world and have a boardroom full of no disrespect to the accountants and lawyers in the room, there's plenty of you here. But a board of accountants and lawyers, if you look at how we connect to each other, there is nothing we do, we can't even walk into our driveway and start out cars without relying on a whole bunch of technology to get where we are. And when that technology fails. It is catastrophic. It underpins everything we do now. And not having a technology person on your governance team and thinking strategically about the organization, I think is absolutely careless. It is flying blind. And it is exposing yourselves to enormous risk. You need somebody with that skill set on

your board. Now I think it is it is well past time. And now, you know part of my role as a technology leader is to bring technology people up to scratch with their commercial knowledge to be effective at a board level and understand governance issues and be able to approach challenges in the boardroom from that perspective. But I think if there's nothing else that you take from this talk today, if you don't have someone with tech experience on your board, you need to address that and address it quickly. So yeah, I think that affects not only the way that we think about risk, but I think it leaves us open to serious strategy blunders. And I see that quite often in the clients that we work with, I work with a bunch of clients that are scale up product development companies that are bringing new products to market very rapidly and commercializing innovations and new technology very rapidly. And where they've got a board without technology input. And it was one I was working with just last week, they've got a board of you know, that represents customer that represents marketing that represents finance that represents operations. Yet, a third of their workforce is technology, people building a technology product, and they don't have a CTO, they don't have someone from Tech representing so I think that's a serious strategy blunder. So let's dive into the Maersk example.

So the NotPetya attack was in 2018. And as best that they can work out, it was people in Russia, looking to destabilize organizations operating out of the Ukraine. So it was a very targeted sovereign attack. The impact that it had globally, though, was absolutely spectacular. So the article sort of starts with this, it's, it's told through the perspective of a an IT worker called Henrik Jensen, not his real name. And he's operating it, you know, the IT help desk in the gift shop downstairs at the Copenhagen head office of Maersk. And it starts with you know, just a normal day sun shining outside, he's got his coffee and in rolls, you know, the first person who's got a blank black screen on their laptop, that read, you know, repairing file system, see, and then a couple of other people turn up and you know, and their screens were also black with this red lettering and and that said, you know, oops, your important files are encrypted and demanding a payment of $300 worth of Bitcoin to decrypt them. What had happened and the article goes deep into this and may get a little bit technical for some of you, but it's worth persevering is they exploited a vulnerability in a very common software package like Microsoft, something like that that's widely used across many organizations. And this organization have been able to find and exploit a part of that software now Maersk lost everything. It corrupted all of their files so spectacularly that it took everything offline that had tech people running around the building, you know, running into meeting rooms in the middle of conferences, pulling, you know, plugs out of walls to try and disconnect from the network that was infecting everything, you know, your network is how all of your technology devices are linked. So, you know, Henrik talks about having to just go home, like there was literally no work that they could do they there was a few managers who kept people in their offices and made them sit there staring at blank walls. But everybody else effectively went home. And he talks a little bit further into the article about, you know, he's sitting there eating his marmalade on toast and having his, you know, coffee in the morning, and he gets a phone call. And it's from the senior tech folk at Maersk, and they say, get on a plane to London, right now, pack your gear get to London. And what they had set up was a war room effectively, like a 24 seven war room in the London Maersk offices, two floors of the building 200 people from Deloitte had been given a blank check to fix this problem. And 400 people from across the IT operations at Maersk, eventually what they found, and I might get this part of the story slightly wrong. But this is you know why it's worth diving into the article,

they found that the one of the offices in Ghana had experienced an outage when the attack was taking place. So there was one image of the company's global systems on one disk in the Ghana office. And then they had this fantastic relay, because the office folk from Ghana couldn't fly direct to London, because of visas, so they had to fly somewhere else and meet somebody else, and then fly somewhere else to get this one disc that had the ability to regenerate all of Maersk systems on it. And from that they were able to rebuild the organization. But you can imagine, you know, they're a global shipping organization, and part of the article talks about at one dock, the next morning, the line of trucks trying to drop off cargo, where they had no visibility over what the bookings were there had no visibility over their customers and where those bookings needed to go and, and how that was all managed, you know, they fell back into this kind of paper trail way of managing that, can you just imagine for one second, and I've told that story to the best of my recall. But when you're reading the article, and having a think about it now, just imagine how you would feel sitting in the boardroom of Maersk, while they were experiencing that.

80,000 people unable to work, like shut down whole organizations, businesses, ultimately, that NotPetya hack cost mask over $300 million. It's not a large sum, when you think about the scale of the disruption and the amount of time they're offline for and the disruption to their brand and reputation and their customers and, and lost merchandise that ended up in dockyards and shipping containers. That attack wasn't even targeted at Maersk. That was just some Russian state based actors trying to mess with people in the Ukraine and organizations that operate in the Ukraine. And that was one of the suggestions by the journalists that may be actually the people who launched this attack didn't really understand the extent and the damage that it would cause. But that's the kind of stuff we're dealing with every day, every day. It's happening all the time. You know, it takes a little bit of guts to say, but China and Russia have invested staggering amounts of energy and resource into cyber warfare. And it is a new Cold War. It is an arms race. It's about protecting yourself as best that you can, but also recognizing that diligence and pragmatism and agility are your best defenses in this brave new world. So just to recap, what a cyber or a data breach can cause you know, you're looking at staff beneficiaries, donors, personally identifiable information, financial information, research and development, all of your secure information being at risk. You're talking about an enormous disruption to core operations and services to recover from a breach. So imagine having to down tools on everything else that's going on in your organization. Just to fix this, like the interruption is almost unfathomable and you're exposing your organization and its management to liability. You're talking about tarnish to brand org and reputation. So cyber attacks are nasty things if you caught up in them, not fun. So that's the table stakes ladies of the game that we're playing now. So get a technology person on your board, be aware of data privacy and regulation. In Australia, we've got a notifiable data breach scheme, which requires you to disclose if you've lost personally identifiable information that's worth a read and getting your head around if you're a director as part of your fiduciary duty. And the big global regulation is the GDPR, which is the European regulation for Where are my notes, the general data privacy regulation, that's pretty stringent and pretty full on if you're compliant with the GDPR, you're pretty safe, you're pretty happy. So questions to ask at your next board meeting. This is a way to unpack where you're at currently, you want to ask if we have the capacity and or capability to protect our staff, customers and stakeholders from malicious digital attacks, that'll open Pandora's box of, you know, what policies do you have in place? What work have you done today? What assessments have you done today? What insurance is is in place,

what your technology strategy is, what your approaches to patching and operations? And the second question you want to ask is, are we are we ready to meet the increasingly stringent data privacy standards and regulations. So that's GDPR. And in Australia, the notifiable data breach scheme. Now, here is your cheat sheet. Take a couple of notes on this one, I think there's five things that we can do in the boardroom being protected from cyber attacks, it's a bit like safe sex, you know, you wear a condom, use barrier protection, you know, you're not 100% safe, you're not going to be perfectly protected, but you're going to be a hell of a lot more protected than you would be if you were just running around without barrier protection at all. So do these five things. And you'll be about 80% of the way there, or at least you won't be exposing yourself to opportunistic attacks and silly stuff that we don't, you know, we don't want to have to deal with. So this is the cheat sheet? Do we have multi factor authentication, protecting our systems with personally identifiable information? Personally, it's a huge flag to me anywhere I go. Now, if I'm accessing important information, and it's not protected by multi factor authentication, that's a big red flag for me. Do you monitor your network environments? That's just a question for the CTO or the head technology person, you know, what, what network monitoring do we have in place? If they are, you know, nothing? Well, okay, you need to know what your network traffic is doing so that you can keep an eye on it for when things go wrong. We need training for staff and employees. And this is one where we can have a massive impact almost immediately. I can't remember the last time in an organization, I had cyber security training, I can't remember the last time we had a foe attack one of my old clients, they would send phishing emails around the network deliberately about every three months to see what kind of response rate they got from a phishing email, for those who don't know, is an email that is it looks innocuous, but it's actually designed to access some of your personal information might be your dog's name, your birthday, your mom's maiden name, all these sorts of things that tend to be used in passwords and usernames. So what? That's a question for the boardroom, what training are we doing with staff and employees across the team around cybersecurity, because it needs to be continual, this isn't a set and forget play. Remember, this is an arms race that we're in, and things change. So we need to be diligent and consistent. On to number four on your cheat sheet is a vulnerability assessment. So this is where you find a nice, lovely, helpful security partner most likely, and bring them in to assess your vulnerability. Don't let perfection stand in the way of good, you don't need to be perfect. You just need to tackle the major things to keep yourself safe. what you've learned from the vulnerability assessment, and from the ongoing training for staff and employees and from managing your network environments, after you've been put in place multi factor authentication, is how does this affect our policies and our procedures and our insurance. That's really where you know, the core and the genesis of how we protect ourselves should be documented on behalf of the organization. So to wrap up, get going start the conversation, we need to be talking about this in the boardroom. And we need to be building a sense of urgency across the whole organization, management at all levels across all functions, that this is a responsibility for everybody. It's not just the IT folks that have to keep us safe you assess the current state and pick a framework. The National Institute of Standards and Technology, which is out of the states has a great cybersecurity governance framework that helps you look at your organization through a whole bunch of lenses that will give you a roadmap to safety. It will highlight what you need to work on first, and why you need to remediate first and get in place to be safe, or to be as safe, as you know, as is pragmatic and realistic. Build a roadmap to resilience. Again, think about your cheat sheet, you know, two factor authentication. Do you monitor your networks? Have you got ongoing training for the team? You know, social engineering and phishing are two of the

most common attack avenues for hackers to access systems. What policies and procedures and insurance do you have in place? And do you have a disaster recovery process? And then prioritize and tackle these items until you feel comfortable that you are resilient? And don't let striving for perfection get in the way of good enough? How's that?

Helga Svendsen 20:43

That is awesome. Thank you, Hannah. So first question, how can small organizations maintain cyber security in a cost effective way?

Hannah Browne 20:55

Yeah, great question, I would look at the size and scale of the partners that you choose. So think about who use for email. So one of the most common ones Microsoft or Google, really, like don't try to set up your own productivity tools, workspaces, that kind of thing. I mean, I'm a big fan of Apple products, because they've got end to end encryption, making sensible decisions around even message groups. I mean, I'm personally not a part of the Facebook community because I disagree ethically with their business. So I don't use Facebook Messenger or WhatsApp, and I try to stay off Instagram. But I do use Signal and Telegram for a lot of my conversations. And I was horrified at my last organization, when I found out that the board that I was reporting to primarily communicated via WhatsApp, I think there was appalling. Facebook is a known collaborator with the NSA, we know that they share every piece of data they own with the American government, so it can spy on citizens at home and abroad. Why would you want to share all of your sensitive board information and financials and tricky people issues that are happening in the organization with a company like Facebook, you know, if you're going to use a messaging app, as a board member, or even in a leadership group, or even amongst your friends, use an app, like Signal or Telegram, you know, they've got end to end encryption, you can have secret chats and sacred groups, you can have like disappearing messages, you know, where you set that all the messages are deleted within a week, you know, this is hyper sensitive information for your organization. So, the board members need to be set up as a member of the organization they need. I have a Greenpeace email address. I'm a member of the organization and my board papers. And the work that comes goes to my Greenpeace address, one of the other people on the nominations committee with Helga and I, we asked her to set up a separate email address so that confidential nominations committee information wasn't going to her work, email and shared amongst her her employees network. So think about the systems that you use, think about those companies track records, in terms of security and encryption. You know, Microsoft isn't my favorite, to be honest, they've built shitty software for a really long time that gets exploited all the time. My personal preferences, the G Suite, that's what I use in my business. And I'm not saying that that's the right answer for everybody. But that's what that's the lens that you need to question when when you're looking at what systems are we on? Is this the right partner for us? And if you want to get super hardcore about it, you know, there's systems like proton mail, and there's productivity suites of tools that are set up for, you know, journalists and whistleblowers, and they're a little bit more difficult to use. They don't have the usability that an Apple product does. But they're much, much more secure.

Helga Svendsen 23:53

Next one in the list. If Maersk had a tech person on their board, how might things have been different?

Hannah Browne 24:00

I'm sure they did have a tech person on the board. Actually, I haven't had a look at that. But they clearly didn't have the disaster recovery in place and addresses this in the article, the way that their disaster recovery was set up was under the assumption that not every instance of every part of the business would be taken offline at the same time. It was a bit of a perfect storm for them in terms of how that attack, the NotPetya attack vector worked. That it it targeted, you know, what was the Achilles heel of their strategy. So what they did was, you know, rolling the big guns, basically, they wrote a blank check to Deloitte and said, get this sorted for us. Yeah, I'm not sure that they could have done anything different because there's no glaring holes in their disaster recovery from my read of the situation. I certainly think that were relatively well protected and they still suffered, you know, a staggering loss of of systems.

Helga Svendsen 25:00

Okay, the next one. And it's been asked by a couple of people in different ways Tech's very broad, what kind of tech experience is most relevant for the board? And then I think somebody else, yeah, what's the particular flavor of technologist would be most beneficial and architect cyber, what what's best?

Hannah Browne 25:19

Look, you won't get a cyber security person just putting that out there. They're rare as hen's teeth. And they're extraordinarily expensive and very, very busy. So you'd be unlikely to find anyone who's actually been in cybersecurity. But someone who's got a depth of experience working in technology, delivering technology, overseeing technology teams, they've just been in the ecosystem in a way that gives them a depth of understanding and capability. So I think the answer to that question is much more about what's relevant for you as an organization. And maybe I'm going to be slightly disparaging of all of my comrades and colleagues, techie people can be a bit awkward, a bit nerdy, a bit weird. That's why I love them. That's why I play in the technology space, so much. Finding tech people with the commercial skills to be useful at a governance level in your organization is probably the more important thing to focus on. Take people who have the understanding of commercial realities of you know, profit and loss and optimization and risk and strategy. That's what you want to think about. So I would look at, do you have a depth of experience in the tech landscape? You know, I'm not talking about, you know, someone who was a primary school teacher, and then who became, you know, moved into software development. Three years ago, I'm talking about somebody

who spent 10-15 years building technology solutions, overseeing technology solutions, delivering technology solutions in organizations. And if you can find someone with that caliber of experience, who also has, you know, an understanding of risk, and strategy and finance and people, then that's someone who's going to add a lot of value to your board. And just to address one other question that came up along the way is, is around upskilling other board members? The way I do it, is I share articles with the Greenpeace board, you know, I am the tech person on the Greenpeace board. And when something interesting is happening in the tech landscape, I share that with the rest of the board. After this talk, I'll share with you a PowerPoint deck from a cybersecurity workshop that we ran for non executive directors and board members. And on the 29th of January without my company, midnight city that talks about the regulatory frameworks, it talks about the vulnerability assessments, it talks about how you want to think about this stuff in a lot greater detail. So I'll share that with everybody here. When we ran that talk, a whole bunch of my colleagues from the Greenpeace board came along.

Helga Svendsen 27:54

So Dominique asks and it's connected to this question about training and upskilling. Are there any short training videos available that we can circulate along with that other information as well?

Hannah Browne 28:05

A look there'd be plenty of I'll happily have a little bit of a peruse? Yeah, I'm just thinking about, like the YouTube channels that I enjoy watching. I wonder if there's one on cybersecurity, where they're, you know, deconstructing and analyzing recent attacks. And I'm sure someone's making funny videos about that somewhere that would be useful to all of us to have a bit of a look

Guest 28:25

And Helga, can I offer on one of my boards, we get all the directors to do regular short online cybersecurity video watching things and then a short test. So two a month and the company, it's a bit daggering, you know, thinner, I can but it's not bad security shift. I can't recall how much the service costs, but I actually think they try and make it funny. So if you do actually find it memorable.

Helga Svendsen 28:52

Great. Could you send that to me Tanya? And I'll include that in the follow up email. That'd be fantastic. Thank you. How do you talk about the sorts of people that you should get in the boardroom? We've got a couple of questions here, one from Janice, and from Fiona, basically the same, how do we get them? How do we attract someone with a tech background? And once we've attracted them, how do we select the right one? And once we've attracted them, how do we select the right one?

Hannah Browne 29:17

I think advertising in a broad range of channels is important. I think go to the places where tech people gather. I don't know if anyone's active in the meetup saying so like advertising in the right spot, connecting with humans looking at the skills and expertise but you know, I would say as the chair in the nominations committee at Greenpeace, that the other major major factor to think about is culture, you know, are their values aligned to your organizational values? You know, are they going to be engaged? Are they going to add? They're going to contribute something that's diverse and is different to what the voices you've already got in the boardroom? Is their contribution going to be meaningful? That would be what I think is the most efficient thing to evaluate, because everyone's going to go about this different and there's no right way to be secure in your new technology stack. So having somebody who you want to work with, in those potentially very difficult situations, the culture bit for me is probably the most important part.

Helga Svendsen 30:19

I'm going to try and sneak into more Hannah. Marg, this is your question about board members protecting information they receive, I can't see you. But if you're around, yep, you're off mute, if you can ask your question.

Unknown Speaker 30:32

Okay, so we receive information individually, many of us get it on computers even more on this thing? How do we know that what we've got, our systems are secure. So the information we receive, how do I know that my AVG virus protector free or my mobile is safe? What should I be doing as a board member to ensure that my own systems computer and phone are safe for the information I receive, and also the information I received doesn't infect my own information and systems.

Hannah Browne 31:08

I personally don't use antivirus or, or, or those kinds of things. But I do take very pragmatic steps. So I have a passcode lock on my phone. And I would encourage everybody to have similar, the most important thing that I did in the last five years towards my own personal security was to start using a password manager. They're a real pain in the butt, I won't lie, I won't sugarcoat it for you there. And like, I took two days in my life to set up my password manager in the first instance, and then run through everything that I have the username and password for and change them all too hard to break passwords, the password managers to use this only to LastPass is the one I use. And I pay for that. Because I think, you know, it's 50 bucks a year or whatever. And like, I don't want that service for free. Because you know, you're getting charged somewhere along the lines. And if it's free to you, then they're selling your data to somebody else. And I don't really want my passwords and usernames sold to somebody else. And OnePass is the other one. So LastPass and OnePass

(1Password) total nightmare, like you want to set aside a day of your life to set them up. But once you have them in place, you have done as much as you should be expected to do to secure your data and your access. If you really want to have a little bit of fun. And this actually went around the board at Greenpeace in the last two weeks. Jump on "Have I Been Pwned", that is a website that records all of the data hacks and privacy breaches that have happened ever. And you can register on there. And they will actually send you an SMS or an email when there's been a breach that affects you so that you find out straight away and you can go and change your username and password. Because we know that these databases of usernames and passwords get hacked, they end up on the dark web and people buy them to try and exploit identity theft or fraud or ransomware attacks to get money out of people. So "Have I Been Pwned"Helga, maybe we can pop that in the in the send out as well. He's also something to use. But for me, the the password manager is is the key. Everybody should use one, particularly if we're operating in, you know, roles like non executive board director and such, we do have important information that is super, super critical to keep private. So we should all be using a password manager,

Helga Svendsen 33:41

Hannah. Amazing. Thank you so much for sharing in the podcast initially, and for sharing here today and for continuing to share straight after this with the rest of the questions that have been asked as well. So that is just magnificent. Thank you so much. Again, if you could just join me in thanking Hannah for sharing all her incredible wisdom. Thank you all for being here today and part of this event. And you will hear from me soon about the next one or of course on the podcast. So if you're not subscribed, I encourage you to do so. Fabulous. Thank you folks, thank you for being here today and see you all soon. And but Henry, if you can stay on the line. Thanks, folks.