Emergent Risk - A Perspective for Super Boards Transcript

Sharmaine Tan 0:00

Well, very exciting to have all of you join us here during your lunchtime. You know, welcome to our live session on emerging risk and this is organized by the cyber data risk managers. So my name is Sharmaine Tan, and I am the executive advisor for Privasec. I work closely with like the chief information security officers to help bridge their business gaps. But I'm glad to be a host here for today. And before we start, we would just like to begin by acknowledging the Gadigal people of the Eora nation and the traditional custodians of the land on which we gather today and pay our respects to the elders past and present. We extend the respect to the Aboriginals and Torres Strait Islander peoples here today as well. And Michelle, you would like to say a few words too?

Michelle Beveridge 0:45

Yes, thank you Sharmaine and I just want to extend what you have said to also recognize the people of the Kulin nation to represent quite a wide spread of Melbourne people on the call as well. And again, extend my respect to elders past and present, and any Aboriginal and Torres Strait Islanders who may be with us today.

Sharmaine Tan 1:05

Thank you. So, thank you Meena for first of all inviting us to your show. So, for those who don't know Meena, Meena Wahi is a director at Cyberdatarisk managers and she's a recognized digital risk insurance expert. Perhaps, Meena in a sentence or two, you can tell join us and our listeners here today briefly about what do you what do you do and what does the company do before I move on to introduce the rest of the panel?

Meena Wahi 1:30

Sure, thank you, Sharmaine. So, we like to be at the forefront of understanding risk as it is evolving, and helping our clients procure the right insurance policies. So therefore, we have very good relationships with insurance companies all over the world, and we understand risk. So, we try to match our client's needs and the risk with the right insurance policies.

Sharmaine Tan 1:56

Excellent. Thanks a lot Meena. And I'm really excited because we have a very, very experienced panel here with us today as we are going to be diving into the different perspectives for Super Boards. So we also have with us Teresa Dyson and she has a broad portfolio of directorships including being a Non-Executive Director, and the Audit and Risk committee chair of Seven West Media for those who recognize the name

and Genex Power. Teresa is also the director of Consolidated Tin Mines, Energy Queensland, Energy Super, Power and Water Corporation and the Gold Coast Hospital Health Board just to name a few. It's quite a mouthful. Do you want to share about anything or highlight some of the interesting work you've been working on?

Teresa Dyson 2:43

Thanks Sharmaine. It's a pleasure to be here. So I do have a sort of group of different sort of types of industries that are in my portfolio in the finance sector, which is I suppose most relevant for today. Energy Super is an industry superfund. We've got about a billion dollars of funds under management about 45,000 members. And as you said, I chaired the audit and risk and compliance committee for that, as well as being an executive director. Just also, I suppose, in the finance sector that might be relevant. I'm on the board of the National Housing Finance and Investment Corporation, which is a federal government body that probably was originally set up to fund investment into community housing projects. And then we issue bonds out into the debt capital markets. Most recently, we've just done a $350 billion debt. That's our third bond raising. And they've been administering the first home loan deposit scheme as of the 1st of January. So that involves quite a lot of interaction and most of it in a digital sort of space between us and all of the retail banks that have been able to offer those first home loan deposit guarantees to first time investors, which is pretty exciting. And the other one in the finance sort of space is that almost on the Foreign Investment Review Board, so we have a look at sort of all of the investment that comes into Australia to an international economy that we have. So there's a lot of focus that we have at that level on data and cyber issues, just from an investment perspective, but also in the way that all the investment sort of fits together as well. So but it's an issue that applies across all of the sectors that I'm involved with as well.

Sharmaine Tan 4:24

Wow. Excellent. Thanks, Teresa. And we next up we have Romain Rallu, who is the CEO of Privasec and also the same company I represent. So Romain is very renowned in our industry for his expertise in the governance risk and compliance space. He has an extensive experience in establishing and implementing Information Security strategies, frameworks, governance architectures for both medium and large organizations in APEC and Europe. He also gets invited regularly to run like boardroom workshops, assisting many varied operational business teams. Romain do you want to add anything?

Romain Rallu 5:01

Yeah, just in short, well, first happy to be here, of course, just to say that Privasec is now, I want to have six offices throughout Southeast Asia and Australia and you said it all I think, actually.

Sharmaine Tan 5:16

No worries. Yeah. It's been an incredibly busy season for us. Actually, I might add, we have a lot of demand for like the GRC consulting audits, technical insurance, drone security. It's crazy. So anyway, really good to have you on the panel with us. And the last but not least, definitely incredible lady, we have Michelle Beveridge, she's an experienced C level executive and board director for more than 15 years. So Michelle is a CIO at Interpid group, and the director and chair in various boards, including Rei Superannuation fund, Vernet, Australian Computer Society and the Queen Victoria women's centers dress. So Michelle skills and practice actually has contributed a lot to revenue and EBITDA, growth and long term sustainability. In the past, Michelle has initiated and implemented significant business change programs. And she was named as CIO 50 Awards in 2016 and 2018. Michelle, anything else you will love to add and share with us today?

Michelle Beveridge 6:20

Thank you, Sharmaine. I don't think there's much more I can add to that lovely introduction. Thank you. I think similar to Teresa; I'm making that transition to full portfolio career. So my Chief Information Officer role at Intrepid is actually no more Thank you to COVID-19. But I think that years of experience in information technology, and looking at the issues we're going to be talking about today, and to the conversation, as well as nearly three years on Rei supers board, which looks at the real estate industry specialist in that industry. And I'm actually Deputy Chair of that board now. So that's been a thrilling change as well.

Sharmaine Tan 7:07

Thank you very much for sharing that, Michelle. And you know, before we're going to dive into today's topics, right, for those because we have a lot of experienced people here on the panel, if you have any questions as well, feel free to type that in the chat box, and I will be going through the questions later and we will have to have some time for q&a. Okay. All right. So we're just gonna dive straight into this now, as we explore how is the financial services sector managing risk, you know, given that there's always new risks that emerge and sees, so how are the boards of superfunds determining which risks will be dominant in the next five years? So maybe, perhaps Michelle, you can kick it off by sharing some of the emerging risks and challenges of the boards in managing them.

Michelle Beveridge 7:52

Thank you, Sharmaine. I think the certainly for every board risk is one of the key things that the boards need to consider. And that's no different in the superannuation industry, the COVID-19, of course, is the big topic of conversation at the moment. And for superfunds, it's the long term impacts of COVID, as well as the short term changes that we've had to make to the operations. You know, things like the early release payment program that's on at the moment that has a long term impact on member outcomes. So we're really looking at, you know, how can we help our members ensure they do have long term superannuation, as well as you know, helping them through the current crisis? There's also things like, increased regulatory attention. We've had the banking royal commissions, we've had, you know, more

and more compliance requirements coming through from the regulators. And that becomes a bit of a balance risk for the superannuation funds, because all that additional compliance requirement means that, you know, it's more administration cost, and you want to make sure that the costs don't get too high compared with the benefits of that regulation. So we're constantly looking at that side of things as well.

Sharmaine Tan 9:09

Meena and Rollain, do you have anything else you want to add to that?

Romain Rallu 9:13

No. In fact, for my side is from a cyber-perspective. Cyber Security has now seen this trailer for the last five years have been a strong topic. Nobody would argue that it's not a risk or not something for the business to consider. It used to be buried under IT, but it's, it is no more. I think what we're seeing is the appetite for board to understand or to the maturity and appreciating cyber risk has evolved. And we work with a number of supers and SSI clients. And what I'm seeing is that when they define the risk appetite to begin a yearly basis, I'm seeing a greater appreciation from the board to try and understand really what cyber risk means to the business. And I've even can think of one as the Super, where the CEO took the chairman to a cyber-security conference in Singapore before COVID-19. And for the chairman of the board to be able to take a couple of days off and attend the conference to educate himself was brilliant.

Meena Wahi 10:18

Yeah, I agree, I think how we were defining cyber risk, and the other emergent risk is shifting now as this risk become more mainstream or dominant risk, and how you treat emergent risk, sort of also changes as those risks become more dominant, and you'd learn to live with them and see them as more, you know, day to day race, you know, so I think super funds and financial services sector have been at the forefront of adopting digital infrastructures and digital infrastructure. If you sort of understand what it means is really operations and customer experience combined over the internet to deliver superior value, right? And once you do that, you start looking at boundaries shifting. But then comes the conversation around reputational risk, you know, data privacy risk, and even online fraud becomes part of the conversation. So, so you know, by virtue of adopting a new strategy boards now also have to accept the risk that comes with it with adopting digital strategies. And I think therefore, we see more emergent risk being part of the conversation and these risks are different, and they need different kinds of treatments.

Romain Rallu 11:42

It's a very good point around emergent. When we say emergent risks, we are trying to look at fast changing risk or fast evolving risk. Is when the case that like you mentioned, that reputational risk, particularly as it relates to cyber, the market perception of what is acceptable and not acceptable for a company has changed dramatically, right. So five years ago somebody got well 10 years ago suddenly got breach didn't understand what it meant to you, then you found a completely unacceptable. And now people fail to

realize that it's a fact of life, it's unavoidable. All you can try and do is minimize it and stop you know, companies on their response to the breach, and not so much focusing on blaming the breach itself. So, so the landscape, the point I was trying to make is the landscape is changing really fast. And risk that's emerging is also very fast changing seem to appreciate it, but also continuously step on top of it, because the the market expectations do shift very quickly as well.

Sharmaine Tan 12:35

Yeah, that's a very good point. And maybe Teresa, why don't you address the next one, right? Have organizations in the financial services sector become more accepting of risk? Not just in particular to cyber risk, but how do they go about in terms of defining their risk appetite, you know, what's your take on this?

Teresa Dyson 12:54

So I think there has been a lot of attention on risk. Generally, it's always been a key feature of what boards are supposed to do. But I think the understanding of the tradeoffs and the balances between risks that you prepared to take to enable you to do business, to be able to increase your different sort of offering, I mean, moving into digital platforms is a risk in on itself. But if you don't, then you're paralyzed in terms of doing business. So you have to sort of understand what the balance is in terms of risk that you're willing to take, and you know, what mitigations, and what factors you can put in place that will manage it to a level that you're comfortable with, particularly in the super industry, and more broadly, the finance industry, because the nature of a lot of the businesses as a custodian for other people and looking after other people's money. There's usually a very low risk appetite that sort of strains across a lot of the activity because you know, where you might have a commercial business that might be willing to you know, take have bit of a better handle on something because the opportunity might be very large. But you know, understanding the risk might be large, when you're looking after other people's money as their custodian, and particularly when it is going to fund their life in retirement, then I think it is a much lower risk appetite that is typical across the board. But that doesn't mean that super funds again need to sort of standstill and not be able to develop business operations that suit the times and that make the service to members because it's all about members first and members interests at the core of all the decisions. So just it's just a balance and I think that boards generally becoming more sophisticated about and more mature about having those discussions and understanding what the tradeoffs and the differences are.

Michelle Beveridge 14:46

If I can add to that Sharmaine as well I think I have seen the difference with superannuation boards compared to other you know kind of more commercial if you like, boards because the attention to risk Rei super is much heavier, in that, you know, low to medium appetite to risk. The whole board goes through the risk framework, at least annually in detail. The risk, there's a data kind of risk committee, which quarterly goes through the risks, we've just in fact finished doing the annual review of the risk framework. So it's right up to date with all the COVID-19 kind of risks in there. Yeah, it's a big part of the financial services industry.

Sharmaine Tan 15:33

That's really good to know.

Romain Rallu 15:35

We're also saying that there was about to just set up the that's exactly what we see as well. When we look at the thoroughness and the with which, you know, different lines, lines of assurance are being set up in nfsi clients, have a much better maturity and risk and control so Risk and Audit find a balance there. And whereas a lot of guessing on financial prices don't necessarily have that level of appreciation. But it goes back down to what Theresa was saying around having a low risk appetite. And I think it's critical that people, you can only afford the low risk appetite when you really understand the risks you're taking. And I've seen I think, in few years ago was I was seeing people stating they had low risk appetite, but really not really fully understanding, appreciating what it meant and not realizing that they actually have risks that they had that were significantly above their risk appetite.

Sharmaine Tan 16:29

True Meena do you want to add a different perspective to this?

Meena Wahi 16:32

Um, I think I will disagree just a bit because I feel that by virtue of accepting digital strategies, businesses in general also become accepting of risk because when you transact online, and you conduct a whole lot of activities and have interfaces that are online, you require a greater diligence of the risk and therefore, your risk management strategies have to be more sophisticated. However, by adopting something new like digital, you are taking the leap of faith by saying yes, we do accept a level of risk by doing so. So, you know, your professed risk appetite may be low, ought to be which is right. But in a sense by adopting a certain strategy, you do accept the inherent risk, which may be higher than before.

Sharmaine Tan 17:30

And we talked about a bit about opera. So, like, you know, a price we know is important guidelines and greater responsibility on board members. So, be interested to hear from the rest of you. What are your experience when it comes to complying with, you know, the Prudential standard CPS theory for information security. So, Teresa, you want to go first?

Teresa Dyson 17:50

Sure. So, we've been closely tracking CPS 234 Now, since it was announced and obviously now that it's official up and running as of this month. So it's been certainly something that we've had internal teams

working on, but also it has featured in a board deliberations and at the audit compliance and risk committee that I chair. We've just completed an internal audit on our compliance with CPS 234. And I suppose our readiness to continue to evolve with it. So which came out, well, it was pleasing from a board perspective. But a lot of work has gone into that as well. And, you know, we sort of very mindful of the fact that, you know, we use third party providers with third party administrators. So it's not just our organization that has to be vigilant in relation to the way that we manage data. And, you know, CPS 234 gives us a framework to measure ourselves against that, but we also have to extend that in our contracts and in our reviews, and discussions with their third party providers to make sure that you know there's not a weak link in the chain and some of the providers are not quite up to scratch with the same level of diligence around complying.

Sharmaine Tan 19:14

Very well said, Teresa, I know Romain you have lots to talk about.

Romain Rallu 19:20

Yes, because it's close to my heart six years ago with a conference in a Gold Coast. And there was about you know, let's give it the gun 50 let's say senior IT manager. And I said that situation security was something that was going to get hotter, etc. And I was almost booed off the stage. Right. So nobody cared back then. And so we have press done is really making that a requirement for people. I think I'm frustrated because it scares people. It's weak in the sense that it is still a little bit of confusion around what level is just required by a prop. When you read the CPS, it's not always immediate to people who don't have a lot of experience. We certainly see a rise in the trying to analyze, like Teresa mentioned, the service that we deliver, what we're seeing now is for vendors that are being inundated with, you know, intelligence assessment and security assessments. And so and we on both sides, because we do it on behalf of our clients, and then we also respond to them on behalf of our clients. So it's raised the bar significantly. I think it's, I think, a bit more information. I think the market will mature over the next year or so as to where exactly is the bar to meet. But I think it's been a huge positive impact in the market from my perspective, not saying that because commercially, we sell the services. I mean, because supply chain was just, it was an easy way to add sources forget that people always pass on the fact that they still remain accountable, even though they've transferred the risk. I think that that reminds them that needs to be accountable to do something about it.

Sharmaine Tan 20:49

Thanks, Roman. But Michelle what's your observation though, and your experience with that?

Michelle Beveridge 20:54

It sounds very similar to what Teresa and Romain have just said. I mean, certainly we went through the cycle. journey in terms of looking at the 234, doing our gap analysis to see what the what we needed to

fix, a lot of it was around documentation and getting the right policies in place. Again, we did an internal audit, we've got it now as part of our standard internal audit plan to have a look at the things that we've got in place and make sure that we're keeping compliant with the standard but even going beyond so that you've got that whole risk culture and Information security embedded into the organization, including the directors, we run regular security tests, you know, the old spam tests and those sort of things with the directors. And, you know, it's a timely reminder that it's actually everybody's accountability for information security right through to the chairman. So when we been on a very similar journey.

Romain Rallu 21:53

You mentioned spam, as Michelle noted before was a company in the US founded by Kevin Mitnick who was in one of the earliest and most famous sort of hacker, right? In layman's term, it's now valued at over a billion dollars, right. And it's a company that sends phishing emails primarily aimed at executives. So it tells you where the market is doing and there's a growing appreciation that humans are easy to exploit the machine in many cases and people are definitely targeting people in order to position executive positions because traditionally, they have been less aware than other people in the organization. So, uh, but it was a small segue.

Sharmaine Tan 22:33

I'm actually quite encouraged sharing the conversation in your share experience because it shows that you know, there has been this talk in amongst like the cyber industry where they feel like okay, board members board chairman's and I really need to, you know, we need to be talking more about cyber risk in the boardroom, right not just risk as a whole and, and to hear your articulate, that's all going to add your understanding and it just shows that you know, a lot more changed and evolved over the years when now this is seen as a really important thing as well. And I'm speaking about that. I'm just wondering why do you feel that the bots of super boards. Do they have skills and diversity for ensuring risk oversight of digital risk? Teresa, Michelle, pre for both of you.

Michelle Beveridge 23:22

Well, okay, I'll go because it's very relevant to my position on the Rei super board. I was actually recruited because it was recognized from our skills matrix, that there was a gap in terms of understanding of technology and cybersecurity. So you know, they did an executive search and after the appropriate due diligence, I was appointed to the board. So very much that making sure the diversity is there. I think the other thing that's interesting for us and I'm sure Teresa's boards are the same, is a lot of directors have that whole lifelong learning as part of their sort of DNA nowadays, it is actually a requirement of boards to do a certain level of training. But I find my fellow directors are constantly sending me little articles about everything from the, you know, climate change to the property market to, you know, superannuation issues to cyber security. So there's this constant lifelong learning and sharing of knowledge across the board and that's essential for this space.

Sharmaine Tan 24:26

That's really good to know. So either

Teresa Dyson 24:28

Yeah, I know guys support that. I mean, I think having a skills matrix that you do, sort of make sure that you've got a mix of different experiences and different expertise at the board level is important. We don't have we haven't gone through that process of appointing someone specifically with the digital experience. You know, we, as Michelle has said, everyone's very committed to the ongoing learning but you know, we're sort of also very encouraging all board members to challenge to ask questions to you know, we're all sort of having experiences across all of our other commitments boards or executives in the case of something other board members. So I think we were able to sort of see that depth of, of things that are going on. And, you know, we've got, obviously internal so there's perhaps a bit of a different approach, that that we've sort of taken in terms of just making sure that we're informed enough to be able to ask the robust and challenging questions and then have a discussion about how we mitigate without necessarily knowing all the technicalities, as much as Michelle does.

Romain Rallu 25:39

Can I just add something that may not be very popular? I think the short answer to your question, Charmaine, is that there is room for diversity. And I think that in the, in the financial services industry, what I'm seeing sometimes innocently, you know, the perception from us being provided to that industry is that there's room as well for that candidates that don't necessarily have years and years of experience, they do have very relevant technical experience. And sometimes I feel that members are appointed because when there is an executive search, like Michelle mentioned, the first thing reproducible go is search for another board member. So sometimes it's staying in the same pool of pool of people. And I think that it's good that's to be able to recognize that I'm on things like digital and cyber security, you do need people that have current knowledge and expertise. And if they can be a board member, they have been one that's fantastic, but it won't always be the case.

Meena Wahi 26:36

Actually, it's a good comment because I'm completing my company director comes from the AICD at the moment and obviously hoping to get on boards. I did I have joined a bank branch or Bendigo Bank as a community branch network and I'm on the board of one of those branches now, but the point that I'm trying to make is that I decided to take up and go on that path because a few of my friends who are non-executive directors would meet me and ask me questions and say, Oh, you know, I'm having a board meeting and we what should I be, you know, what do you think can be discussed? And I was giving them points like, you know, ask a question around supply chain risk. And if, you know, you have discussed ownership of liability and rates across the supply chain with your contractors, so answering so many of these conversations, and I thought, oh, boards must, you know, boards must have a gap in terms of skills around technical and cyber, and it seems in seems to be correct. I think there's definitely a gap there.

Sharmaine Tan 27:46

Yes, and hopefully more of this sort of conversations will help to bridge the gap, you know, and bring it bring a raise a certain level of awareness as well. But before I move on to the next question that I wanted to ask you Meena, I would also just want to open this session up to the floor like the rest of you, as you're hearing, all that has been discussed. I'm sure there's questions that's coming to your mind as well. So feel free to take advantage of that and, you know, keep your questions coming, and we will get to them in a bit. Okay, so, back to you, Meena, I really thought it'd be good for our audience to hear about, like your experience, specifically, when it comes to risk transfer mechanisms for treating risk. So, you know, what do you think cyber insurance should provide cover for? Because that's your area of expertise. And, you know, do you get multiple reinstatement on policies and coverage for digital supply chain risk?

Meena Wahi 28:39

Yes. So the one thing has to be clearly understood is that insurance is a treatment or a mechanism for transferring residual risk. Insurance companies all over the world would not accept risk of a business that hasn't gone through the conversation and the compliance around expectations of managing risk. So, you know, like Teresa and Michelle have spoken about how they've carried out the risk assessment exercises, said the risk appetites. That's actually a very critical process when it comes to risk transfer because we like to see evidence of all that having happened. And the conformance to CPS, CPS 234 is evidence and posture of a business that is compliant and manages risk. And we recognize that there's always a percentage of risk that's left, which, you know, you can't mitigate or manage but can be transferred or else some businesses might just like to accept that risk and not, you know, transfer it to a third party, who's an insurance provider. So when we take on risk, especially when it comes to directors and officer's liability risk and cyber risk, the evidence of that performs part of the conversation. So somebody like me you understand cyber risk, would like to have an in depth conversation and find out what the business is doing. But also, we like to alert businesses and super funds and financial services sector businesses to the fact that, you know, there's emergent risk in terms of online financial crime. What about issue around loss of customers and contracts if there is a cyber-incident because you are a custodian of third party data and third party funds, but if they go missing because you have outsourced third party data, your customer's data, your customer's funds to a third party and the third party loses, you know, the funds or the data, then your customers will hold you responsible and you lose the contracts. So some of the progressive insurance companies from London are actually insuring for reputational loss and under that they cover loss of contracts. Loss of customers and they there's a lump sum payment around that, which is very progressive. They are also covering for supply chain risk, which is that any data that's lost by a third party, they would actually consider that as your loss. And the policy will trigger as you would have, perhaps had a breach within your infrastructure as opposed to a third party infrastructure. And there's a greater recognition that you know, privacy legislations which are global in nature may trigger so you can't hold an Australian business insured. We can't just keep a business insured for local privacy legislations, but the global privacy legislations are now covered by a number of progressive insurance policies, but we like to see the corresponding DNO directors and officer's policy cover and the BI policy power as well that a business has. So we can see that they talk to each other.

Sharmaine Tan 32:02

Michelle and Romaine do you want to add anything to this.

Michelle Beveridge 32:07

I think certainly from a cyber-insurance, Meena's got a huge future for her business because there is such variation in the policies out there and a huge variation in price. It's, you know, they've come a long way in the last four or five years, we've had cyber insurance for five years. And what we're seeing now is very different to what we saw five years ago. But it's still a very murky market to try and figure out where to go and who to go with.

Romain Rallu 32:35

Yeah, I can only second that and I think that people used to initially when it came to the market people fully have a silver bullet sometimes. But it's part of the essential baseline fabric of controls you need to have. And trying to subscribe to policy of a good brokerage is just madness, because there's so many variations, so many maturities in the market, and we see sometimes different questionnaires asked by the insurers to the potential insured. And you can see the huge variation, the majority of the questions been asked, you still have people going with free questions like, do you have antivirus? Which means what exactly right? It's just such a broad, silly question. And people have a much better appreciation it of salaries and what it really means awaking really hits. So yeah, I wholeheartedly agree with what Michelle just said. And Meena is right in saying the word progressive, it is really about progressive insurances are the ones who are going to win this market appeal.

Teresa Dyson 33:34

I'll just add one extra thing to that. I mean, I think the level of maturity of the product is certainly changed since I've sort of been watching it. I mean, at first, it was really a bit more treated as a subset of crime insurance or proceeds of crime that just you thought somebody might, you know, steal some money and, you know, you'd have to put a claim in and get it back well, you know, divert it to a, you know, Brazilian bank account or something and that was sort of as far as people thought. Those questionnaires that you mentioned, I know, certainly in a couple of businesses that I'm in, you know, they're going as far as really testing the human vulnerabilities and the sort of training that, that you have at the individual level, what's what sort of, you know, verifications and, you know, read events and hackings, you sort of do to sort of try and do that, but, you know, really sort of targeting the training in relation to, you know, phishing and, and you're just clicking on things or multi factor authentication, you know, just the vulnerability of passwords and things. So all of those sorts of things now are being very being elevated in, in businesses, not only because the business just doesn't want to go through a cyber-attack, but you know, it's becoming important in terms of the level and type of insurances that they're able to access.

Roamine 34:51

Yeah, I think part of the discussions that I have with usually senior executives when I do awareness sessions and, and so workshops like this is people who have breach usually say we don't want to have a breach again. And I say with tough luck, you're going to have one, it's just unavoidable. It's like me saying I don't want to fall sick again, I will fall sick again, all I can do is boost my immune system. Have my emergency number sorted says it's all about the response. And my general fitness, right? Which is not the best conceited. But anyways, the point being that, but yet it's about breaches do happen, and we just can't. It's a dangerous approach.

Sharmaine Tan 35:37

All right and we actually have a question that came in from the audience. So thank you, Andrew. So his question is that, you know, it's fairly well accepted that COVID-19 was on and beta in the risk management frameworks, and then he wants to find out from the panel, what do you guys think about like a pandemic plan, planning right? Would it now be incorporated in risk planning practices and processes and frameworks? Maybe if you can just share a bit more detail about how you think that's gonna pan out.

Romain Rallu 36:11

So maybe I just have a first stab at this because I feel quick question on the topic. Planning for scenario specific planning is getting harder and harder. And if instead you break down your business in terms of assets, tangible or intangible that can be impacted and levels of impact, you can almost read out a scenario trigger your responses. So pandemic planning is different than any other sort of scenario planning. The question is, what is impacting me in my business, what functions and methods do I lose?

Teresa Dyson 36:46

I was slightly different sort of take on as well as I mean, I think, you know, all businesses had business continuity plans, you know, VCM management and I think prior to this global event people thought they would pretty much cover anything and to a large extent, very internal sort of looking. They were effective. I mean, certainly now in Energy Super use as an example, you know, we had a very effective plan to, to get people off site and all that sort of thing. So that was part of our business continuity and, you know, backups of information. What I think wasn't contemplated was the combination of the global impact, the impact on the economy, you know, complete shutdowns of cities and states and countries. So I think, to that extent, it's different. I mean, I think after the GFC, everybody just started thinking what happens if we have, you know, international market volatility of that sort of nature again, you know, that's one thing to plan for, you know, having to get all the people out of an office for a short or long term. That's another thing to plan for when you're planning for those two things, plus all of the other impacts that we've had no regulation, law change on the run, you know, just all of that sort of stuff I think most businesses I'm involved with are having a bit more of a broader look at whether it's called pandemic or whatever it is, but some sort of broader risk that incorporates, you know, a few things happening all at once and with a pretty, you know, globally devastating sort of impact.

Michelle Beveridge 38:23

I mean, in Rei super it's, it's, it was almost serendipitous in that we had just finished doing a review of a business continuity plans. And we had, you know, beefed up the pandemic in there because it's mentioned in some of the, the effort documentation. So we decided to do a test of our pandemic plan just before COVID hit Australia. So we, I know, we had the staff working from home we yeah, we tried the whole, you know, just notifying the staff the night before to say don't come into work tomorrow, work from home, so on We went through the whole scenario playing, and then COVID hit Australia. So we basically say, well stay there, you know, it's working, staying home. And I've not been back to the office since. So it was just one of those things that we were a little bit lucky. But definitely comes back to that, you know, reviewing stuff constantly looking at what could potentially be out there. And then testing it.

Sharmaine Tan 39:25

A little foresight actually. Because, like, you never know when this is going to be useful for you. In fact, one of my conversations with this size or the state of Michigan, I think about more than 10 over years ago, he was involved in coming up with the pandemic playbook for H1N1 virus and that was incredibly useful now because now the government in the US is actually using that playbook for COVID-19. So you never know, you know, when we talk about planning, VCP and all that that's actually really crucial to always look at all the different aspects right and then be prepared. So Romaine when you wanted to say something.

Romain Rallu 40:01

I was about to agree with what was saying there but when Theresa mentioned the magnitude is different, and it's truly a domain to this unprecedented, and it's, and I know the idea that's been a bit with the pandemic, it's something that's an aggregate of impacting issues, but the longevity as well is that's, that's new. So now people have realized that, you know, it's the new norm YT is going to be the new norm for the foreseeable future for the next, at least for the next 6 months to 12 months. Some large companies saying we know returning to the office, some people have canceled the lease options on the levels for the officers because some people are saying the office becoming more of a hangout. So, it's really funny because we do a lot of policy work and when we look at policies, so inside governance of companies, we moving things away from BCPS and our plans to put them into acceptable use and working from home and, and blurring the line between working from home is not part of acceptable use because it's such a such a common occurrence. But there's a you know that that, that so I think when we look at including is, what if my incidence firmly changes the way that I do business? It is one of the question. It's interesting to see what comes out of this.

Michelle Beveridge 41:12

It's all about agility, isn't it? I mean, you really got to, you know, our business continuity management team originally was meeting on a weekly basis to make sure we were addressing stuff hasn't changed.

Now, they started to three weekly now, but we still kept that group going, because, you know, we see it's changing every day with what's happening in Victoria, you wouldn't have imagined, you know, a month ago. So, you know, you just got to keep being agile.

Meena Wahi 41:42

True, and also coverage for business continuity laws. You know, it's time based in insurance policies. So some of my clients have insured for three months, you know, because they thought or business interruption would last for three months. Some of the health practices that can't function had three months or six months, because you imagine you can only be shot for a short while if there's a fire. But now they're learning that, you know, you have to have business continuity loss for 12 months, maybe just to add to results, it means point that the length of the disruption is much.

Romain Rallu 42:15

It was very telling when they extend just keep it to the end of March, right? If you say, well, that's the most expensive measure of one of the most expensive measures so, so they have no interest in extending it beyond necessary. So the fact that this time around they gave it such a such a big run, tells you where we know what the government is being told when listening to the experts and advisors.

Sharmaine Tan 42:39

And you know what, there's a lot of interesting questions that have come in. So I'm hoping we can cover all of them, but we will try to attack them as much as possible. So there's one that came in from Neil Plummer. Thanks for that and he actually want to express his thanks to the panel because he's really enjoying the discussion. So he wants to dive in a bit more we talked about earlier about you know, the boards on super fans and their view perhaps over the next five years, you know, when it comes to emerging risk, but he wants to know like, what, how do you see the boards and superfunds reacting on climate change risk over the next few years, particularly with regard to transition risk, and a potential for stranded assets, reputation damage, missing out on lower cost renewables and things like that?

Teresa Dyson 43:23

I think climate change risk has, has certainly taken a bit of a life of its own, I mean, Asik and Abra, both sort of commenting on you know, making sure that people are mindful of it in our most recent risk workshops. So like, Michelle, we have one every year and we had as in June, we made the deliberate decision. So climate change risk had been an emerging risk on our register. So we've moved now into permanent risks and we were grappling with whether it was a standalone risk of itself or if it just featured across multiple other risks. And yeah, we got advice going to try. So we ended up sort of putting specific actions or and risks around climate change across a number of our core risks. So reputation was certainly

investment risk. So I think we're very mindful of the fact that, you know, again, through the lens of members interests first, you know, we've got to think both of the investment returns that are available and not sort of, to necessarily turn ourselves off to things that can provide a return but by the same token, we can invest in something that you know, will have a short life or will ultimately end up you know, with stranded assets or assets that you know, we just can't sell or that become unworkable. So, so we've got a real balance of approach. We are Energy Super which, you know, as an industry fund our prime members electrical and electronic electricity industry, the nominating organization for many years, Energy Queensland, which is electricity distributor. So, yeah, we're very well aware of, you know, the impact of renewables, the impact of retiring coal fire, past power stations and how that all sort of plays into future investment portfolio as well as the broader, you know, ESG sort of risk, you know, we were looking at becoming a PRI signatory, I think, within the next few months. So we're sort of taking on board a number of those elements of that, including climate change, but for our perspective, it's multifaceted. It goes across, you know, probably four of our main 11 risks that we track. But as I said, we've made a deliberate decision that it's not emerging anymore. It is well and truly here and that's the way that we're treating it.

Michelle Beveridge 45:48

Yeah, I couldn't agree more Theresa, we've done the same the climate change has definitely move from emerging to part of the permanent resort we look at. We also look. looking at ESG policy with the last two board meetings, we've been discussing the changes we need to make to that. We're currently doing a product review. So, you know, what do we need to do in terms of member domain for sustainable investments. So starting to look at where that's at, a bit like the energy industry, the real estate industry is not necessarily at the forefront of this area. But definitely we're starting to see some interest. And I think there's also even when you look at COVID-19, and the Black Lives Matter, all those sort of activist movements that are on at the moment, they're all interconnected, because climate change impacts the poorer communities and people of color, those sort of areas, first. So we're seeing that now. And that's the sort of thing that as a risk, you know, we need to be looking at board level.

Sharmaine Tan 46:53

That was an interesting question that Jenny asked, and I'm also really interested in that actually. I'm curious to find out like, what's your observation, right on having set on so many different boards, do you find that there is a trend where it is the board that is leading cybersecurity discussions? Or is it more the executive team that is doing that in your organization's? Where do you think it's coming from, you know, discussions about cybersecurity who's the ones leading this?

Michelle Beveridge 47:18

I think it's a two-way conversation. It's about certainly the directors have been coming more aware, I think reminded identified this and Meena has as well earlier on in the conversation, and that is generating conversations with executive that might not have happened in the past, but equally the executives are up for the questions because they're also looking at it at the same time. So I don't know that I see also, one

particular area started the conversation, but certainly I'm seeing the conversations are happening a lot more than they used to.

Teresa Dyson 47:48

Yeah, I agree. It's a bit of a chicken and egg thing where might have started but certainly all of my boards a standing item to serve understand where we're at. And I suppose some of them, we've been on a bit of an evolving process of, you know, appointing different sort of roles in the executive team that, you know, again, sort of many years ago might have been the IT sort of guy. Now, they, you know, technology offices and things are much broader, and I think, much more have a broader sort of remit in terms of reporting up to the board on these sorts of issues. So, again, I think, you know, the, the board asks the questions and, and can make sure that the relevant executive, you know, muscle power is there to be able to handle what they need to and then to be able to come back to the board. So again, it's, as Michelle said, its two-way.

Meena Wahi 48:56

Um, yeah, I agree with you. I say it's been sort of a two-way conversation. And like Michelle said that the executives have an equal part to play in the conversation. I just feel that there's a bit of a shift because privacy if you if you talk about trust, and you talk about reputation, then the board gets in interested because the shareholders come in and reputation. You know, I mean, after a cyberattack or beat any adverse event, you know, we see the impact on stock prices, etc. So if we feel that the board gets active there because reputational loss and conversations around privacy being a civil right, that getting impacted. The board's want to project a reputation that's responsible because the board you know, the board is responsible, and therefore, we feel you know, with those sort of issues, the board is more active, the board is more vocal, and rightly so. And when we have a conversation around ensuring reputational loss as a standard no laws, we're just more interested in talking to the board because we feel like reputation is owned by the board as an as a risk. So the, from an operational perspective cyber will always have the IT interface and the executive interface from a non-operational and strategic and risk management perspective. They are strands to it which fall within the scope of the board's responsibility. Or maybe you agree to see that.

Romain Rallu 50:32

I wholeheartedly agree, I think that it shows the importance of articulating cyber security matters in a way that makes sense to the business. And that's another thing that I keep preaching right left and center as safely as you can articulate it in a business fashion believe it's not a risk, and sometimes I see people think technology is saying or the specific technology is going to come crashing. And he asked the so what test so what so what so what the method figurations you realize that okay, well, yes, it's something we want to avoid, it probably is a risk that the board is to control. So, back to me this point here, right, the minute we make the connection between service security and assets that the board is there to protect, and to and to develop, then then we have board leaving that conversation, but until we can make that that

relevant connection, and that's on the executive and on the IT team and on the security teams to make that relevant, and it's hard to have that that sort of level of importance is in shifting everybody. Oh, yes it has been shifting with this. We're not gonna feel we're there yet. Particularly outside of the financial services industry, because of what we mentioned earlier, which is the appreciation of risk is not that it's not the same in all industries.

Sharmaine Tan 51:46

They're all set. Yeah. And it's different. I feel like there's a based on what I'm seeing as well in other different conversations. It's, there's a lot of there's an evolving, happening and a change of mindset, but it's taking a while to cross different sectors different countries and he takes conversations like this and conscious effort from the executive team to really try and bridge that gap with the board. And some of the board directors have said, you know, there's only some elements of cyber risk that they understand, right? At the end of the day, because it's such a complex matter is so broad. But you know, what really help if we can, you know, put together something that's a bite sized for them, right, maybe the top 10 things that they need to know about cyber risk, and that will make it so much easier. And that's something that CEOs have requested or board directors have been asking, and maybe that's a discussion for another session. But yeah, that's something that we are seeing, which is really interesting, but we only have time left for just one last question. And just gonna give that to Jamal. He's asking about AML ESG and modern slavery act. They're all in a mix of regulations of super investment sectors. He wants to know what your thoughts and comments.

Teresa Dyson 52:53

Um, so we have a pretty I think it's a pretty robust tracking system that goes through our governance and compliance report that we received that, you know, looks at all of the obligations that we have, particularly the, I suppose the regulatory and ESG, perhaps is the one that's not quite as obvious in that list AML and modern slavery act, you know, we've got legislation to refer to, we track against it very carefully. ESG, again, probably back to some of the comments more on climate change, although it's obviously broader than. And sort of taking in more of the observations about news and the Black Lives Matters and other sorts of more social and economic sort of issues that are going on at the moment, which is why we're sort of looking at signing up to the PRI principles.

Michelle Beveridge 53:48

I don't think I could add to that we are going overtime.

Sharmaine Tan 53:51

Yeah, that's really good to know. And I think we've that we have actually come to the end of the session. I do, I have seen a lot of comments coming in where everyone just Thank you, thanking actually the panels organizer. Thank you Meena, and for all your insight is, yeah, they all say expressing how interesting the

discussion was. I'm so glad to hear that you guys enjoyed it. So thank you very much for staying here with us all the way. And a huge thank you to Meena for organizing this and a big thank you to Romaine, Teresa and Michelle, for your time, like really appreciate your taking time out to just share extensively from all your experience and your observations as well. It has been very, very helpful. Any last words, people?

Michelle Beveridge 54:35

It's been a great conversation. I know every time I do one of these I learned something myself as well. So thank you. It's been good.

Sharmaine Tan 54:40

That's really good to hear that.

Meena Wahi 54:43

Thank you for this. Thank you Romaine. Thanks, Michelle. That was great. together.

Sharmaine Tan 54:47

And thank you, audience for all your questions. Really appreciate it. Thanks, Jenny for staying all the way too. So all right, we'll see you guys again and one of these sessions will make an announcement I'll send you the recording when it's out and in the meantime enjoy the rest of your day ahead. Have a good one. Cheers everybody.

Everyone 55:04

Bye!