Webinar Transcript

The board's role in overseeing cybersecurity and protecting against data breaches

So hi, everybody. Welcome to our webinar today titled the board's role in overseeing cybersecurity and protecting against data breaches. My name is Sean McDonald, and I shall be your moderator for the next forty odd minutes. Firstly, thank you for attending today. We always appreciate the effort you make to be here for our live events.

And during the session, if you have any questions, please use the q and a toolbar. It just enables us to keep a track of all those questions coming in as against the chat. And finally, if you stay through till the end, which we hope you will do, we have a special treat for you as is customary for our webinars.

You will go into the draw for our beautiful gift hamper if you answer our really short one minute survey at the end of the webinar.

Now for those not too familiar with BoardPro, we are a board software provider sometimes called a board portal, and we serve just over thirty five thousand users around the world across about thirty six different countries.

We enable organizations to prepare for and run their board meetings more efficiently and effectively with clever software, delivering with less time and deliver more impact and value for the for the organization.

And as much as we're a board software provider, part of our wider mission is to make the fundamentals of governance free and easy to implement for all organizations, but especially those organizations with resource constraints.

One of the many ways we do this is by providing free access to over two hundred business templates, governance templates, I should say, guides and resources as well, which you will find on the resource page of our website, funnily enough. And these web these, webinars webinars that we run are also a great way of accessing key governance knowledge without necessarily the time commitment and cost of in person events.

So for the next forty odd minutes, just sit back and relax and try and add to the discussion by answering asking asking as many questions as you would like, not answering. The full recording of the webinar will be sent out to you, tomorrow now, which will include a copy of the slide deck and the transcript and also a special white paper that has been put together by Stephen McCrone.

So without further delay, let me, have the team introduce themselves starting with you first, Stephen.

Kia ora, everybody. I'm Stephen Macron. I'm fortunate enough to be working from Sunny Gold Coast this week.

I run a a management consulting company. We specialize in, strategy, risk, and innovation, of course, cybersecurity being, firmly rooted in the risk domain.

We we specialize in working with clients who have very complex or fast changing businesses.

Chris, jump in.

Yeah. Good afternoon, everyone. Chris Lloyd here. I am the cybersecurity manager at Water Care Services Limited, which is the largest water utility in New Zealand. We provide, water and wastewater services to roughly one point eight million people.

My team's responsibilities are really just protecting the Water Care's mission across our corporate systems, our water and wastewater treatment plant systems, and then also our smart sensor networks that we have, around the show. So we've got quite a diverse sort of footprint that, my team are responsible in protecting.

Thanks, guys. Well, let's kick us off. Let me find the next slide, and we shall move on in. Over to you, Steven.

Cool. Thanks, Sean. This slide really, talks about the strategic environment in respect, to risk. And what it really shows is that we have three if we plot frequency and consequence in respect to risk, then we have three or we can have three domains.

Probable risks are things that are likely to happen to us, the generally high frequency, and we can tend to put fairly robust solutions in place. Possible are the things that are a lower number of potentially more serious events, and these are things where typically we respond, by threat hunting, I. E. Looking at the emerging threat and then putting technology tools, training, etc.

In place to deal with the known or the knowable. We have training and we can exercise against known threats. Beyond that, most organizations have a crisis management, process or policy where the emergence of threats that are plausible these are things that we, might call black swans or things that are suddenly upon us before we realize what they are, and we deal with them as catastrophes or as emergencies. And we deal with those through red teaming, which is where we get people to deliberately attack our systems to to show us vulnerability.

We want to develop adaptive capacity, and we want to create what we call human sensor networks to, allow us to become more sensitive to threats as they emerge from the plausible domain.

The, in the field of cybersecurity, we see that a lot of organizations invest, a lot of effort in the probable impossible because these are things that we can see and tend to under invest in creating the adaptive capacity that you use to deal with plausible threat.

Chris, everything sorry.

You can go ahead.

Not on that last slide. No. That was that was great, Steve. This slide here really just talks to, what we call the threat landscape, from two different perspectives. One being so the adversary or the bad guys and and, you know, what personas they might have and and the ways in which they may target our organizations.

But then also the systemic drivers that drive a lot of this adversary type activity.

So WaterCare, we are critical national infrastructure because we provide water, arguably, one of the most, important resources to humankind.

We are, yeah, well, I guess we're lucky enough to have quite a a unique threat profile and and that all of these, adversarial threat actors are somewhat of a, of a focal point for our organization.

So the nation state actors, you know, the, these, these, these bad guys usually look to espionage type tactics, pre positioning within critical infrastructure in times of geopolitical, uplift.

Targeted and opportunistic cybercrime is the majority of of the threat for most organizations.

We have specifically separated these out between opportunistic and targeted. Opportunistic is the spray and pray.

Really just looking for opportunity.

And, yeah, get good things from that. And then the targeted cybercrime, are more capable and credible groups, or organizations of criminals, that have a lot of funding, and a lot of capability behind them.

Steve, did you wanna talk to some of the systemic risks that we've discussed?

I guess what we're seeing, in a in a more global sense, and, you know, a lot of people focusing on artificial intelligence, in respect to both detection, and, I guess, perpetration of, cybercrime is as we're getting more sophisticated technology, as we're getting more interconnected in terms of the types of systems that we use, no one will be, unless you've been, you know, living under a rock, missing the fact that the geopolitical world is becoming more and more volatile, and we're getting, you know, big tech and antiquated technology kind of crashing into each other. And this creates a landscape of threat where it's harder to predict the types of threats that are coming, and it's, there's just more and more of them.

I think a good good point. Sorry. On that last slide, Steve, was really around the AI, enablement aspect. Right?

So, you know, the Western world is a lot slower in adopting AI due to, you know, some of the constraints that we we look to try and solve and and get through some of those challenges around governance and privacy and so on. Whereas, you know, the bad guys, they they don't have that ethical boundary. Right? So they're running really fast at enabling their mission or their operations through AI.

So, you know, we're kind of losing the game a little bit here. Like, they're able to run a lot faster and get outcomes a lot faster as as well. We're seeing a lot of, weaponization, being a lot quicker because they can leverage the likes of artificial intelligence to get that speed and that velocity.

This slide here is, one of the ways that, you know, WaterCare tries to prioritize its approach. So we've been doing cybersecurity now for over a decade, and, you know, we we started off the traditional model of looking to compliance frameworks, best practices, sort of benchmarking ourselves, and then building programs of work out the back of it to really just uplift the areas of where we have the most vulnerability or our processes lack or we we might lack some governance.

And so, you know, over that time, we've built a pretty good benchmark and we're now at a, at a good point where, you know, I would argue most of the opportunistic, or, Yeah. Opportunistic type threat actors are not really a problem for our organization.

Sure. The the holes in the, in the cheese may align from a Swiss cheese model. And we, and we may see ourselves exposed. And that will come down to our ability to, again, like capacity to adapt and sort of respond to those sort of incidents. But we could close those down relatively quickly. What we're more concerned about now are the credible and capable threat actors that exist. And because it's a viable business model, in other parts, not necessarily the Western world, we're getting a lot of uptick of people and organizations coming together and creating quite good capability around cyber to do harm and to do damage to try and get that financial gain.

So what we've done now is we're pivoted to more of a intelligence led threat informed approach. And so this really just takes a different perspective where we're not so we we still look at risk and we still look at compliance for sure. We we will always have that. We need to maintain that.

But what we're trying to do now is look more from the perspective of what are the bad guys doing? What are we seeing left and right? What's happening today? What's happening tomorrow?

And how do we dynamically assess how that might impact us or how that might affect us?

And we're building a capability off to the side of that around being as quick as possible, being as proactive as possible across these threats. So what this, the screen here shows is, an example

of one of the many tools that we use to try and contextualize or sense make all the different bad guys that are out there willing to do bad things to us. Because there's so many, how do we prioritize that? And so there's different metrics that we feed into this, and it gives some pretty good data, data to work off.

Okay.

So on this situation, if you look at the previous slide then, it's easy to become overwhelmed or at least bombarded with, you know, a lot of information, a lot of sort of scary stories about threat, about threat actors, about change, about AI.

And what we try and do, is create a kind of a metaphor or a simile that we can actually talk to senior executives and directors in a way or using a language that they understand. Cybersecurity is about making decisions and those decisions to deploy resources need a kind of a return. So when we think about cybercrime, we think about it as a profitable global enterprise. Cybercriminals, in the largest cybercriminal organizations have, you know, human resource departments, they have marketing, they have finance, and they have boards of directors, they have governance, who are working with these people in order to establish and create a return on the energy that they put into hacking into cybercrime.

And as the photo there shows, this is a police raid on a professional cyber criminal organization and it looks, feels, and acts just like a normal software business.

Okay. So if it's an industry then let's think about cybersecurity as participating in that industry. You cannot create the conditions where you are immune from or cease to participate in that industry unless you want to cease to participate in any web connected device or mobile connected device.

So as as if we look at that as a business, we say okay how do we make ourselves a bad investment? So how do we make our organization an unworthy target from a set of people who need an expectation of return? And We think about that as increasing the cost or the time and energy for cyber criminals to engage with us, decreasing the value or the return that they can expect from that investment, and increasing the value or the utilization of the knowledge and information that we gain from interactions with cyber criminals and believe it or not you are interacting with cyber criminals almost on a daily basis.

So we think about moving from a defensive mode to actually an active mode and the easy parable to think about is you know, there's there's two of us in the savannah and we see a lion. I don't need to outrun a lion, I just need to outrun you. Your organization can't outrun cyber criminals, it just needs to be faster than other organizations in your industry. You need to make yourself a bad investment. The way to do that is to think about it in terms of resilience, and resilience is about maturity and adaptive capacity.

Maturity is about the probable and possible. Adaptive capacity is about dealing with the plausible.

That's very true, Steve. And and, you know, like, if you put that into the context of these criminals looking for their money. Right? Like, they're they're they're looking to earn earn their dollar bills. They want that ROI. So as soon as we make it difficult for them, they are going to move on for the most part, for the opportunistic type cyber criminals, which make up a vast majority of of the threat that sits out there.

And there's also other strategies that you can also do, for more of the targeted and credible. You just need to make it harder for them to do the things that they need to do. And so if you put a lot of perspective across that, it's a different way of thinking. That's it's really just like breaking down how would they be doing this and what can I do to slow them down? Or what could I do to confuse or disorientate or really waste their time? There's all sorts of different really, like, cool strategies when you really break down the problem.

Guys, I have a question in here from Ayesha. It's quite interesting considering our audience, which are primarily small to medium businesses, across Australia and New Zealand.

And she asks, what tools or checklists can help us assess our current levels of cybersecurity?

So if I'm in a small to medium business, I'm a general manager, an owner, or a CEO, what are some of the tools I can use?

Yeah. The it it it is difficult for smaller to medium enterprises because there's just so much to think about. So it's really around that prioritization piece. And so if you were just starting from scratch or the or you're new to to looking at this as a as a problem or a challenge, The New Zealand government and the Australian government give really good recommendations around the quick wins, the things to be focusing about. So, that you've got the Australian, Central eight and we've got the CERT NZ top ten.

You could also put this threat informed approach across it as well. Right? Like what are the bad guys actually doing? So a lot of the threat reporting that comes out of the ACSC, the NCSC, it's all public public reporting.

They talk to the sort of the top trends within the last year. And so putting that into the perspective around your investments. Right? So if this is what the bad guys are doing over the last year, over the last forty eight months, how do I weigh up in terms of having the right controls to stop this sort of thing from happening?

So it's sort of a two pronged attack, right? Like you, you look to a good best practice framework. And again, you like the, the government's provide us this, done some really good work in, in making it usable for small to medium enterprise. But then also, you know, doing a little bit of research around what is happening within my industry, what is happening within, Australia, New Zealand, and how do I translate that to the controls that I'm establishing.

It's actually a good segue, from that question. Chris, I'll I'll throw it to you to introduce the idea of maturity.

Yeah. Okay. So, we've been doing maturity for a very long time. So it's it's sort of how you look at like, how how are we placed in terms of having the right controls to stop bad things from happening, and and you take a maturity based approach in benchmarking and assessing that.

So you look across the controls and you say, look. Is it good? Is it bad? Is it is it fantastic?

What is the metric that we put across this? And then what is our appetite or our tolerance level across this level of risk? And what level do the controls need to be? And then we kind of road map the gap, right, and and try and uplift.

What I found is that once you get to a certain level of maturity, it's an exponential curve of investment time and and money to to get to the next level of maturity.

And my reflection as well around organizations that, have all these compliance frameworks. They have ISO, they have SOC two, they have NIST.

When it comes to capable and credible targeted cybercrime and espionage actors, they're still getting hit. Right?

So it's very dynamic. They the bad guys know the compliance frameworks as well as we do. So they're just going to try and bypass them. Well, they're going to be novel or they're going to be dynamic, and they're just gonna do things to get in. So what we what we've pivoted to is more of a capability approach around how do I build the capacity for my team to be quite dynamic and how do we solve things quickly opposed to going off the old method of assessment, body of work, program, outcome, and it's quite static or quite linear in in motion.

I guess, like, one of the one of the things that, would be a key takeaway is around you you can't really stop all the things from happening, but you can have a business continuity plan, which will address a lot of things around technological outage of which cyber contributes to. So having a good incident response plan, looking at your mission critical services, why does your organization exist?

For for most, it'll be revenue generation, shareholder return. What are the core things within your business that provide that? And what technology supports that? Those are your crown jewels.

Those are your focus. That is your mission. And then you just work backwards from that. And having business continuity plans across that, if that technology fails, how do we still keep delivering the outcomes, of our business and our industry and what we do?

Steven, back to you.

Yeah. I'll just build on that idea, from Chris is is really identifying. So as he said, you know, it's the can be an exponential curve in terms of resource commitment. So if you can really be clear on the systems, the processes, and the information that you need to continue your business, then you would put, you know, eighty percent of your resources into the protection and recovery

of those resources if for any reason they were hacked or, you know, for any other reason a storm event etc.

My kind of go to when I'm thinking about this sort of stuff is, when we had the Christchurch earthquake it was in the days when a lot of people had the server in their office and the server was their key infrastructure and key database for running their business and I know of a number of people who literally risked their lives to go in and save the server. So if you think about it like that, what would you run into an earthquake damage building to save in respect to your mission critical assets? And that's really your start point for, your cyber security.

If you just jump to the the next slide, we'll talk about, yeah, adaptive capacity. So the other so I said and a both and. The other part of, resource commitment is, and I believe, certainly from discussing and working with, Chris at Watercare, that adaptive capacity is the thing that really saves you in an unprecedented or catastrophic event.

If if the bad guys are doing the same thing the same way every time, it would be very easy to defend against. So by definition, the thing that puts you into a catastrophic or crisis will be unique or at least be unique to you.

And what we do with adaptive capacity is we think about it as as just building. We're building knowledge knowledge of the system, knowledge of what's changing, We're building knowledge in terms of the threats that are emerging, knowledge in terms of how other people like us have dealt with those threats. We want to build some skills, that skills in the team to identify and react to the to emerging threat. We want to build abilities, we want to have technology and people who are equipped to deal with that type of stuff. And most of all, we want to have experience. We want to be able to exercise.

We want to be able to test in real time that we can adapt to an emerging threat. And that's not just, people. It's also a process. If you've got to write a business case, wait a month to get a, or wait for a board meeting, or wait for permission to buy something or do something, then you are by definition going to be operating in a slower tempo than the threat actors. And if that's the case, then they will outmaneuver you very, very quickly. So one of the things that we have around adaptive capacity is really being very clear about where permissions lie in terms of spending money and taking action, but also clear about things like how we communicate.

Boards spend a lot of time agonizing over what are we going to say, how are we going to say it, what are we going to hide, what are we gonna retain inside and make sure that no one ever finds out? Okay. Have those discussions, but have them in the context of an exercise or a high pressure, event where you're really feeling the heat. It's easy to say I would never pay a ransom, but actually when the heat is on and you know you're gonna have stakeholders, shareholders, employees, and government having a go at you, then people make different decisions.

So the key there is to really, prepare and then practice.

Chris And and from my experience, tabletop exercises are gold. We run tabletop exercises within water care, once a month, sometimes even twice a month capturing different stakeholder groups, and we just run through scenarios.

So I guess if we put this back into the perspective of smaller organizations, you know, just run through a scenario. There's a lot of really good resources again on the government websites around putting some stuff together, and they've also got some placeholder, references that are already put together for you. And just get the key stakeholders in the room and get some trusted partners. Sit down, have a coffee, run through it, and just talk around how how would you deal and respond and make decisions in in this type of situation.

We've then extended beyond that now as a larger organization. We now simulate. So we started with tabletops. We started with discussions. We discussed, discussed our approach and and made sure that our governance and processes were were good and the decision making matrixes were sound.

Then we wanted to practice it. So we ran full scale simulations across our organization.

And that really and and every time you do this, every time you do it, you're gonna learn something. And that's what it's all about. As well as satisfying some of the things that Steve mentioned before around building that muscle memory and getting people in the zone and thinking around the situation.

Guys, I have a question that's come in here, which is a fact, a question that I was gonna ask, which is most small organizations contract their IT responsibilities to external providers like hosting, storage, accounting, HR, those things.

How do they choose a provider in the context of cybersecurity? Where do they go to find this capability?

So just so I understand the the question right, is this around outsourcing your cybersecurity or, outsourcing your technology functions?

But it's something like in in the context of small business.

Where does someone go to look for assistance in and around cybersecurity?

Yeah. Look. It's, it's always quite challenging, especially in that, small to medium enterprise space.

There's a lot of really good providers across Australia and New Zealand.

There needs to be trust, between you and the organization.

I would suggest maybe having even another third party help you through the process if you can.

But it is difficult and really it just comes down to trust and credibility of the organizations that you're working with. I mean, you can go as far as asking security related questions. So again, there's some really good resources on our government websites around supply chain and third party risk.

And so you could use, you know, and frame some of those questions and, and ask these providers, you know, do, do they do this? Do they do that? What assurances do I have? You could also look at the contractual, side of the house as well and ensuring that, you know, there's liability clauses and expectations within, within the commercials.

But ultimately at the end of the day, it's a risk and, and, and the organization will always own the risk. So it really just comes down to having a plan and, and, and embedding the plan with your third parties and making sure that, you know, the process is understood. If things do go pear shaped, everyone's aware of how how you work together to overcome it.

Yeah.

So, like, an an example would be, let's say you use HubSpot for your CRM. You're not gonna work with HubSpot as an SME on improving their cybersecurity.

You can read their, their policies around that copper stuff, and you can see, what they do in respect to keeping themselves and, the data that we, give to them safe.

But one of the key, principles of of adaptive capacity is is start from where you are. So if we're doing an exercise at AGLX, we do use HubSpot, but we'll do an exercise that says HubSpot is down and we do not have access to our customer data.

How are we going to maintain, communications with our customers? Like, what are we going to do while HubSpot sorts themselves out?

And then we exercise on that.

So it's it's a matter of saying, you know, start from where you are, work with what you can control. I can't control HubSpot. Cybersecurity, I'm fairly convinced, is pretty good, but it's still, you know, potentially it's plausible that it goes down, and therefore we need to have a backup of some degree of how we're gonna manage that. So that's that's really how we do it.

Guys, is there any such thing as cyber insurance for small to medium enterprises?

And and if there is, what's the right level of cover?

It's a good question.

That's highly contextual. I wouldn't be able to answer that. Sorry. That's I already.

I've I work with some insurance companies. I believe you can insure.

I think that's a conversation you would have with your insurance company. I certainly wouldn't make any recommendations.

It's a good, you know, it's a good way to think about cybersecurity in terms of an investment perspective. You'd say, you know, what would be, the likely cost to us of an attack on a certain system or a certain process or if a certain part of our our business went down and then think about that from an insurance perspective. It's probably a good conversation to have with your insurance company.

Another great question that's just come in from John, Steven. John asks, what information should a board be receiving, and what questions should they be asking to give them the necessary comfort around those risks?

Yeah. Actually, we're gonna get to that, soon. There's a there's a couple of slides there that get close to that and I think measures of success.

I've also, in the paper that you guys can download, I've written, not so much questions but considerations at each of those stages. What should the board consider and and what's the type of things they should be talking about? So it's really answered across across that.

Okay. Great.

That's a very good question, so thank you for for asking it.

Moving on.

So with this slide here, we've, we've tried to break down. And again, this is probably aimed more at, a larger enterprise, but can be translated down to, to small to medium enterprise. This is the, the governance architecture that, that some enterprises choose to adopt.

To note here that the top level of authority is done with some form of document. We call it a charter here, but it can be really whatever whatever you wanna call it. But it holds the statement of intent. Why does the cybersecurity capability exist and what is it responsible for? Or how does the organization view cybersecurity and what is the commitment?

And it also defines the authority to act. One of the things that we've learned is that predescribing or predefining certain levels of authority to make decisions really speeds up your ability to respond to bad things, especially if you're practicing it through the likes of tabletops and simulations.

And, you know, for me, it's really just empowering, empowering those, to make those decisions under certain scenarios from a risk perspective, right, within a certain level of risk tolerance.

The strategy really just sets out the, the roadmap, the vision, the intent, the roadmap, and how, cyber and resilience will execute the business mission.

Architecture is the security practices, technologies, and processes. It's the whole gambit, policies. This is interesting. So like a lot of people would see policies as kind of the yes or no thing, right? Like you're allowed to do this and you're not allowed to do that. The way that I see security policies is that it's a left and right of scope. Right?

What is the runway in which the organization can run at delivery, run at doing things within the tolerance level of risk from the organization?

So for me, you know, well drafted, well defined policies are really important. It has the roles and responsibilities of, of people within the organization and what they need to do.

And it trickles down into the standards and the procedures. So the standards are where you align to best practice. So for example, a policy might be, we enforce our technology with multifactor authentication. All technology is enforced by multifactor authentication.

The standard will specify the types of multifactor authentication that is, is acceptable. So it might be SMS. It might be the authenticator app or it might be hardware tokens. And depending on the level of risk or the thing that you're doing, that might change. But what you're doing is you're empowering the organization to make decisions across that.

And the procedures are built from the operational units. So security, aren't pushing security down. It's you run your business unit, you create your own procedures, just make sure that they align with these security standards. And so therefore, you're not you're not sort of like the security yes or no shop. You are guiding the organization to achieve the things that they need to do. So you're embedding security in a good way.

Yeah. The main, point of this slide and this, again, is, larger organizations where the, board of directors and audit and risk committee or through the audit and risk committee if you have one. And really their role is to set the expectations for cybersecurity, and you can express that through risk tolerance. You can express that through, the, a charter or strategic document.

And really there the the main point is that all of the resource commitment in cybersecurity should be directly aligned with the strategic intent or the mission of the organization.

And it's easy for organizations to kind of get lost in cybersecurity in terms of, you know, and ask for big resource commitments and big programs and big technology and lose that that link to the organizational strategy. So really, for me, the board of directors, that's their first and foremost concern.

We want to have, obviously alignment through the risk policy, and then we talk about resource allocation. An important point here is boards should also be very clear with how they're going to share and learn from other organizations. In the past, there's been a real, I guess, focus on keeping quiet when things aren't going right in terms of cyber security. Sometimes that's useful, other times, and particularly now when there's compliance issues around reporting breaches, that becomes very important to really understand how you're going to share and how we're actually going to learn from others.

There could be in many organizations a competitive advantage to be had from good cyber security, so maybe some of the stuff you're doing in terms of deception or some of the stuff you're doing in terms of, critical risk analysis you might want to kind of keep to yourself.

At the at that level, once we've passed that to the executive team, I think to Chris's point, there has to be a lot of trust. There has to be, a lot of understanding of how to build capability, knowledge and skills, etcetera, in the executive team and the and the, cybersecurity team so that you can trust that they are going to get the job done in respect to, the strategic intent. And that's you know, there's a list of things there that we talk about.

Steven, Sarah, asks a good question here around table topping. She says, could you talk a little bit more about tabletop scenario and what type of stakeholders you would involve?

Sure. I mean, maybe Chris could talk if you I came out about some of the examples of things that you've done at WaterCare.

Yeah. So, I mean, you could do it at any level of the organization. The context will be different. So if you're doing it at the at the strategic level of execs and and the board, you'd be looking at around, like, how we're governing this, what decisions need to be made.

I would say focus on how do we make the right decisions faster?

What can we create that will, or what, what kind of documentation templates or artifacts could we create to speed up process?

You know, some of the things that have folded out the back of that, those type of exercises, communication templates, liaison authorities across organizations. So, you know, you might look to engage with a certain, organizational entity at speed. So you just need to have the authority to have an open and transparent communication lines outside of the, the normal ways of doing things, I suppose.

If you're doing it more of at the operational level, it's really just going through technical scenarios, and having technical stakeholders in the room, like the experts and, and just talking through it. And like I said before, it doesn't matter who you get or what, at what level you pitch these tabletops.

You will always learn something. What we haven't run a tabletop yet where we haven't learned something or many things. We we're constantly learning from them. They're a great tool.

Just in respect to that, you know, setting up for a tabletop, you want to learn, how to do, you know, proper debriefs. You want to learn how to do proper, you know, mission briefings, etcetera. So, you know, there's a lot of a lot involved for organizations in terms of how they prepare for and learn from those tabletop exercises.

Can I ask an obvious question which might be a bit silly?

Go on then.

What is a tabletop?

That is a good question.

Excuse me.

So I have a crack at answering that.

It's really just getting stakeholders in the room and running through I think it comes from, like, a gaming methodology. You're playing a game, right? So you're putting yourself in a situation. And there's different ways that you can do these tabletops. You can do it through a discussion based type, facilitation method, or you can get someone to to run it.

There's all sorts of different ways that you can can run it, but really it's just scenario planning in a in a fun, open, transparent way.

At its most basic, you grab a team of people in a whiteboard.

You throw the scenario on the table and say, tomorrow morning, we do not have access to HubSpot. We need to communicate with our clients in a way that kind of makes sense.

Let's go. And then we start to think about who are the who are the people that we're actively engaged with at the moment, who are people that are, etcetera etcetera, and we start to think about, how we might deal with that situation.

And we're just mapping it out. We're saying that won't work. That's only gonna work if these conditions are satisfied. How do we make sure those conditions are ready?

Simon's got the database on his laptop, and he's drunk. Oh my god. What are we gonna do? You know, this sort of stuff. So we just we should be playful with it.

And and I would also suggest, you know, keep the mission in mind, right? Because there's many different tabletops that you can be doing.

Go back to the core objective of your organization and, and your mission, and then work backwards from that, just so you are prioritizing the right thing. Because I have seen in the past, some organizations running tabletops for scenarios where there might be something that they could focus on that would be much more valuable.

Okay.

This is the the last slide. So measures of success, we we steer away from this idea of KPIs. There's no real set of indicators that will tell you everything you need to know about cybersecurity. Remember there's a lot of stuff going on in the plausible domain that you can't see yet, so we think about how do we know that we're kind of heading in the right direction.

You know, the old measures of, you know, how many times we've been attacked, how many times have those attacks been successful are really not that useful.

Although, you know, if you can measure it, obviously, it it does have some utility.

So we we break them into the two things of maturity and adaptive capacity. So for maturity, you can do an assessment, and there was a spider diagram in the earlier slide where you can say this is the expectations as soon in terms of NIST or IEC, how do we stack up against that? And you can have a third party audit you or assess you against those if that's that's your thing. You can benchmark against similar organizations, although I'm always a little bit cautious with that because I say benchmarking against organizations that are dissatisfied with their cyber security may not always be that useful either. But generally it's okay because in a lot of industries they can give you a whole lot of information And it certainly can detect things like, you know, if you're using, you know, pre twenty twenty systems in twenty twenty five, then you are by definition vulnerable and go back to being a bad investment. Well you're no longer a bad investment, you're a target.

The capacity for threat identification. So can we identify emerging threat? Can we bring that understanding of threat into our business in a way where we can make real changes based on that understanding? There's a different thing from knowing the threats there and being able to do something about it. Again, if you've got to wait three to six months to get your business case approved by the finance committee and then go to a multi vendor competitive bid and then select the thing and then apply it, well, you're too slow. So is your you know, are you mature enough to actually be able to deploy those resources quickly against an identified threat and are we regularly testing that?

And those are questions that the board should be asking of the executive. Adaptive capacity, you know, can we work quickly? Are we doing those exercises? Are we actually doing those desktop exercises or, you know, purple teaming where you have your red team and your cyber team working together to really, hit a a plausible scenario or a plausible penetration type test or a plausible set of threats. Are we learning from that? Are we changing systems based on that? And going into this, Chris made a really good point and that is many organizations go through a large technology transformation after they've been hacked.

So just leave it there and say, well, actually, exercise the hack and then go through that transformation before it costs you a lot of money in terms of recovery or a lot of, reputation risk in terms of, the PR that comes out of it.

And your capacity to adapt should be something that is very concerning to the board. Are we getting better at this stuff? Are we actually doing this stuff for real?

Any last comments from you, Krista?

No. Other than, I guess, for the smaller medium enterprise, everything Steve said, but also in the perspective if you're a trusted third party or you're a trusted provider. So all the things that

Steve said are the things that you should be asking them as well around, you know, where are we at and where are we going.

And all that stuff's in the in the paper that you can download.

Great. So that paper, by the way, everybody, will be sent out, tomorrow via email, and it'll also be linked in the resources section of our website under webinar page on the webinar page. Sorry.

So feel free to connect with, Steven and Christopher today. I'm sure they'll look forward to your connection. And if you'd like to connect with either of them, just let us know on the survey at the end.

So you'll receive the email from me tomorrow now, which will include a copy of the, webinar recording, the transcript, the slide deck, and the white paper from Steven. So just as you leave the webinar, don't forget to complete our really short one minute survey going to the draw for our gift hamper. I'll announce the winner for that tomorrow.

Thank you again for your attendance, everybody. I hope you enjoyed the session. Our next webinar is on May sixteenth, at the usual time of one PM New Zealand time, eleven o'clock Australia time. And the topic is AI generated board minutes, tech savvy, tech or risky business.

And that is with, Helen Van Orton and Danica McLean. So So if you're considering using AI for your board governance, then this webinar is definitely for you.

So thank you again, Steve and Christopher, for the great conversation today. Really appreciate it. I look forward to seeing you everybody at our next webinar. Have a great day.