Untitled - April 29, 2026

Speaker This podcast episode is brought to you by Kordia your trusted advisor and cyber security and resilience national sponsor of the Institute of Directors. In a cyber incident, you don't know who's in there. You don't know how bad they are. You don't know how long they've been in there. You actually don't know what you're dealing with. The NTSC has noted that of all the attacks in New Zealand that possibly of national significance, a third of those were nation state attackers. That would be China or Russia or Iran or any of those countries. The technology is changing at a fast pace. We can see with AI coming in and sophistication of the attacks. So it's really important that directors are clear that boards are given some really clear direction about what's required of them. My involvement was really, you know, providing national support to the district health board at the time. And, you know, there'll be all sorts of views on how well, you know, people felt that they managed that. And at the time they didn't have a board, they had commissioners. There are a lot of unknowns, and it is impossible to protect against all kinds of attack. If you talk to the then chief executive at the time, he will certainly be able to share with you what it was like for him. But it was the first. And, you know, he would suggest only time he ever wants to go through it because it was massive. Directors are operating in an environment with so many distractions that could lead them to take their eye off cyber security. You're listening to Board Talk Off the Cuff, and I'm your host and producer, Sonya Yee. Cyber attacks can leave a company or organization at a standstill, with services shutting down, leading to a long term loss of public trust. And in the case of the health system, huge potential for patient harm. But how big are the risks and how much should boards invest in cyber security measures. Is there a one size fits all and what does proper due diligence look like? I headed out to Central Wellington to meet Patrick Sharpe from Kordia to find out more. Hello, Patrick. Lovely to meet you. Oh. Thank you. So on this side of the office, we have Kordia team. So these guys work all kinds of radio engineers and IP engineers and that sort of thing. And then through here we have your side of the office. So these are where all our security team works. So security consultants, cloud consultants, that sort of thing as well. Patrick is a general manager at Aura Information Security. He's been there for almost a decade. So let's just say he's seen a lot in terms of how cyber is shifting and the different ways hackers are looking to infiltrate systems. So aura is the cyber security consulting division of Kordia. And so we focus on providing advice and guidance to businesses as well as penetration testing. So ethical hacking. These functions are sort of audit functions. So they sit outside the day to day operations of a business. So for that reason, we have order or as a separate advisory, like a hacker will illegally hack into something in order to extort money out of someone. Whereas companies pay us to use the same techniques to demonstrate what vulnerabilities actually exist, and then emulate them and tell them what they are so they can fix them. What have you discovered? There are all kinds of things. On occasions, we've actually found enough vulnerabilities in applications that they've shut down the entire project and stopped it. But for a lot of things, there's a design flaws and code bugs. So mistakes made when they're deploying things or mistakes made in the design process. So when you say they're deploying things like who the heck is companies, government departments through this door is where all those files are hidden. Yeah, yeah, yeah. And this is our awards. These ones are for the best security company of the year. And these one, these two gold ones are a bit old,

but this silver one is fairly recent. Now, for the uninitiated, when it comes to technology, what's the difference between a cyber incident and a cyber breach. So cyber crime is obviously a criminal activity through cyber lens. A cyber incident is any kind of incident that involves that sort of space, right. A breach is probably more specifically about loss of data. And we're seeing that in the news happen more and more. But is that because businesses are not prepared or they're just finding other ways in? There is a combination. Some of the businesses that have been hacked offshore have actually been quite prepared, but have still had major incidents. But also companies in New Zealand are frequently not prepared enough and are not reacting well enough to a cyber breach, potentially demonstrating potentially a level of negligence. We are very used to in New Zealand, thinking about twelve zero zero zero mile sea border, right, and thinking no one's going to bother to attack us. But you can get anywhere in the world in fifty milliseconds. That's one fifth of the length of the time it takes to blink. So in terms of our vulnerability as a country. Are we prepared enough? And how do geopolitics play into risk for us as a nation? But when it comes to actually being attacked. Attackers are not looking at a globe and saying, well, look, what's this down at the bottom? What they're doing is they're saying, I'm scanning a lot of IP addresses or internet addresses, and they all look the same. And they're looking at Western countries. They're looking at who's the Five Eyes. New Zealand's flag looks very similar to Australia's and Britain's. We are part of a bloc of countries from an external perspective. So we are going to be targeted. You know, for a long time we've had this global rules based order and that's starting to fragment quite a lot, as I'm sure you've seen with international wars and that sort of thing. And that has an immediate impact on cyber security or cyber crime. When you actually look at the Iran war, a lot of the intelligence that they've got from that is from hacking the street cameras and working out a map of Tehran. There are ongoing hacks. And the thing is, two hacks aren't exactly new. The first hacks on critical infrastructure around the world was in the two thousand, and it was called Stuxnet. And this was an attack by America on Iranian nuclear centrifuges to try and destroy those. And it was detected in the wild. And people saw it and understood what it was going on. But there are now there's now malware out there that is specifically targeting machines that are in the Iranian time zone or using Farsi as a default language when it comes to, obviously, the global threat landscape in general. It's becoming much more balkanized, and that's affecting cybersecurity quite a lot. Well, the Gcsb have talked about New Zealand businesses being attacked by hacktivists based on Ukraine war issues. And so if one of the one of our organisations does gets hacked by them, it might be just to disable them. It might be just to make a statement. They might not be trying to get money or sabotage or espionage or anything like that. But equally Chinese government has attacked the American government and American telcos and American energy companies and critical infrastructure for espionage and sabotage purposes. For the hackers. It's bringing in the cash so our businesses and organizations have a lot to lose. Cybercrime is costing New Zealand about one point six billion dollars a year, and the direct impact on New Zealand businesses is more in the realm of in the millions and the twelve or so million. I think it is. So those seem like quite big number differences. One of them is, I think, how much companies are paying out in ransoms and that sort of thing. But the actual impact on those businesses in terms of having to rebuild infrastructure, re-establish trust, uh, loss of revenue, those sorts of things, really adds up. Boards understand the importance of protecting the organisations they serve, but with cybercrime, coughing up the cash behind

closed doors doesn't get you off the hook. Our survey actually shows that forty three percent of businesses who were threatened with a ransom in the last year did pay that ransom. We certainly don't recommend it because it continues to fund cybercrime as long as people are paying ransoms. Cyber criminals are going to keep doing what they're doing, but sometimes they think a business doesn't have a choice. They say we're either in business or we pay the ransom. What could you do before getting to that point? There's a lot you can do. First of all, to protect your data, but to make sure it's backed up and that you actually know that you can restore it. If you have good backups and the ability to restore it, then their ability to hold a ransom over you is much lower. A third of companies in our survey recently said that they didn't think they could actually survive a major breach, and that's exactly why there's no room for boards to be complacent. And yet, the stats might tell us otherwise. The recent director sentiment survey is really talking about increasing the amount of involvement of directors within technology, within organizations. But the number of boards that are talking about cybersecurity at a board level has actually plateaued for the last three years. But why do you think that is? Yeah, I don't know. It's possible that the forty percent of boards who are not thinking about security think it doesn't apply to them, or possibly they have directors who are not maybe not as many independent directors. And so they tend to be a bit more, um, thinking in their bubble. A lot of the sentiment from the executives who were in our survey actually talked to use fairly complacent terms. It's never happened to us. We've been in business for fifty years now. If we compare where we're at to the rest of the world, New Zealand definitely isn't where we should be. We are actually sixtieth in the world when it comes to regulation, which is way below the other partners in the Five Eyes, which is Canada, who's number two? Australia who's number twenty one? We sit just below Rwanda and Egypt. But our technical adoption, our adoption of technology is much further ahead than theirs. So our ranking on that scale puts us in a really strange position. It's largely because the government hasn't legislated about it in the last couple of years, whereas other countries have. So Canada and Australia and the UK have put a lot of energy into legislating and now have a really robust legislative scheme, which generally do hold directors criminally liable. If there is an incident, then and there's negligence. So directors, your time to act is now. There are a lot of unknowns and it is impossible to protect against all kinds of attack. But the you can still have a clear understanding of what risks you have, and be doing your best to minimise those risks down to an acceptable level within within a business budgets and. Okay. But what's how much is too much? Well, that's a very good question. So that's why it's really important to actually make sure that you have security experts, um, alongside you, helping you make those decisions. Having worked in this field for about a decade, Patrick is well aware of the different ways hackers are getting in the back door or even creating doors of their own. Attackers are clearly becoming more bold and more. They're targeting much bigger groups, much bigger companies, and going for much bigger paydays. And you can see that in the attacks on the entire aviation sector in America, the entire retail sector in the UK. Companies like Asahi, they took out thirty factories for a couple of weeks. The other one is um as AI tools are really help create impersonation tools, they used to create really convincing social engineering through email, through voice and through video. And these can be used as ways of getting into companies. But does it mean nothing in the cyber world surprises. Patrick. Now, there are many things that I've come across in the last ten years that have made me really sit up and

pay attention. One of them I remember was when one business had two cyber incidents right up at Christmas time. They were always at Christmas time. Both of them were impacting their business in a huge way. And so they were running around really trying to work out how to actually continue their business, which was a critical provider of health services. And that's exactly why directors can't take their eye off the ball. Complacency at any point is, is the risk. One of the other areas which always really surprised me was that in twenty twenty two, Australia had a number of data breaches. One was Medibank data breach and the other one was the Latitude Finance one. It's a parent company of Gem Finance in New Zealand. And at that point Australia said, well, this is not a good situation. We need to become a world leader in cybersecurity. And New Zealand didn't really make the papers. And so here we are now, three, four years later and New Zealand is way behind where we need to be against the rest of the world. It's fair to say the stakes are high. There are numerous risks for boards. One of them is choosing not to act. Due diligence and governance best practice are key, and the Institute of Directors is working hard to put measures in place for boards, and that includes protecting them against regulatory changes around liability. Well, boards play a really big role in setting a culture and expectations with stakeholders and helping to build the trust. And, you know, cybersecurity is part of that. Stakeholders want to know that when they hand over data or, you know, that it's going to be treated sensitively in accordance with the regulations and inappropriately, the board needs to be aware of that. I'm Susan Cuthbert, I'm principal advisor here at the IoD. So I've been putting together a submission around the proposals that the Dpmc have put out. That's Department of Prime Minister and Cabinet around the cybersecurity of critical infrastructure. It's essentially reform across a number of key sectors that are important to New Zealand. I mean, there's huge liability involved for directors, is that right? So the regime imposes some very serious really significant obligations, has a component in it where it's talking about holding directors personally liable to ensure that certain obligations are carried out. It's not government policy at the moment. So it's relatively early stage, which is great because directors can consider what's being proposed and actually look to shape some of this stuff. But rest assured, changes won't be happening overnight. There's going to be a bit of a process around which organisations are considered critical, which organisations fit within this regime and those that won't. It's about upping standards, organisations working closely with the government so that we can ensure that we have good national security within New Zealand. What were some of the things from a policy regulation perspective that were red flags? It's the breadth of the regime. Boards are involved in this space. They need to be aware of the extent of the obligations that will be imposed upon the entity, and also at a personal level, I'm directors. So it's really important that boards look at what's being proposed and kind of asking themselves in practice, can we really bring this to life? Will this work with our systems, with the capability that we have around the board, around the level of capability we have in the organization? What are the requirements around investing and upgrading? What is that going to really look like in terms of the assets that we currently have and where we really need to get to in order to satisfy the regulator? So it's all those really practical issues that need to be considered. So we need really strong engagement from boards at this stage. So that good policy is actually developed because there are requirements. They talk about voluntary information sharing, but they also talk about mandatory. They talk about incident reporting. There may be situations like if there was a really serious cyber event, it may be that, you know,

the minister actually wants to intervene. So it's all those sorts of powers that we need to really think through what that would mean for an organization who may have commercial interests, or who may be subject to other regulators requirements as well, with the mandatory and voluntary information sharing, is that these kinds of things that are going to hamper directors from either understanding the parameters or does it create confusion? You know, the technology is changing at a fast pace. We can see with AI coming in and the sophistication of the attacks. So it's really important that boards are given some really clear direction about what's required of them. The other component that is within this set of proposals is to make directors personally liable. Criminal liability. So it's pretty serious stuff here, but it's not just talking about willful misconduct or intentional wrongdoing. The concern that maybe we have, and we think this really needs to be unpacked is where it starts to talk about where the directors have acted reasonably or even recklessly, because we have to take into account that directors actually do have to take risk. Really standard part of governance practice. So we don't want them being held liable for, you know, doing their best acting in good faith. So we have to make sure that the settings are are right and that they actually encourage good governance and encourage directors and boards to do the right thing and to really cooperate with others and to ensure that this national cause is supported. Which brings me to the director sentiment survey, which Patrick Sharpe from Kordia mentioned earlier. So from Susan's perspective, is that because directors don't know whether the yardstick is long or short? It's probably fair to say that we can only go so far with the voluntary regime, particularly given the circumstances of what's happening internationally and the tax that already happening on New Zealand. So we can't afford to be naive around this. You'd expect there to be some minimum standards in place. But we also have to think about, you know, how do we bring about good results when it comes to governance? And a part of that is ensuring that directors are very clear around the expectations. Those expectations have to be settled, and they have to be clear so that directors know the direction that they're heading in. So what's the IoD looking to achieve by putting the submission together, and what do directors who know nothing about cyber need to think about as a first port of call? Well, first of all, we want to teach people about governance. Boards provide a great deal of value to an organisation through their function. But we also want people to understand that there are some limitations as to what directors can control or be aware of. Cyber security needs to be on the agenda for board discussion. It can't stay within the organisation at a sort of IT or techie level, it needs to be considered right across the organization. If an organization feels that they don't have the capability in-house to advise them, they need to get external advisors and they need to be thinking about where do they sit on a maturity curve and where do they need to get to and over what period of time. We want the main compliance duty to be put onto the entity because that's what makes sense. You know, that's where the implementation happens. That's where things can really go wrong. Boards need to be held accountable for their duty of providing oversight. Being really clear about the different roles that the board plays versus management as well. The other thing that we're really interested in seeing is, is making sure that the proportionate approach to liability is truly proportionate, so that directors aren't being held liable for acting in good faith, doing what they, at the time considered was the right thing to do, because there's this thing called the tyranny of hindsight. It's very easy to identify risks and talk about what should have happened in terms of investment or actions after the fact. But at the time, because of the complexity and

the fast moving components of the system, it can be really difficult to work out what's right. We need to get them right so that directors feel like they can really support the cause that they're being called to do in terms of national security. We don't want to get these issues around liability in the way boards need to be respected for the contribution they make. There needs to be a level of trust there that they will do the right thing and come to the party on these matters. The cyber criminals, as they'll call them, they're fundamentally lazy people who want to find an easy way in and make a buck. It's big business out there. Company director Shane Hunter. In the health domain, there's a price for health information, and it's higher than it is for certain other information, you know, to be able to access that information and make money or, you know, perhaps there's a bad actor that's looking to get access to VIP information, you know, their loved ones, if you can make the connection. So it's an area of great interest and, you know, health, seeing an increasing number of attempts and successful attacks globally, I think all organizations need to be risk aware when it comes to cyber. When I worked for IBM in the eighties, we used to run the national health system. There was actually a single national system. Information security or cyber security just didn't exist. Shane's firsthand experience of dealing with cyber breaches saw him assist toward a compass, a p h o based in Wellington and the Waikato DHB, through his role as deputy director general data and digital for the Ministry of Health. I find health and incredibly addictive space. It's in part helping people get better or improving health outcomes. I just find it really meaningful and that I can connect with it. I've got my own sort of personal stories and family stories, and where I've seen the system underperform and you know, where I'd like to make a difference. And worked in district health boards, you know, the pharmacy sector and primary care and, and now the private sector. And so, yeah, it's very interesting when you look at it from the different parts of the system, how much better it could be if it was better joined up. Yeah. Just a space full of huge opportunity. And I think that that really appeals. It's a place where you can have impact. So just what it means for, for people in New Zealand, but protecting New Zealand, let alone your stakeholders, becomes incredibly challenging when your data's been hacked. You know, we have, like most organizations have some sort of a computer outage of some sort, a network outage of some sort. You generally have a sense of what's going on. You know, you start relying on people diagnosing and, you know, resolving. You can get back to business as soon as possible. And a cyber incident, you do get, oh my gosh, because you don't know who's in there. You don't know how bad they are. You don't know how long they've been in there. You actually don't know what you're dealing with. You know, they can ransomware you they could be lying. You just don't know what's going on. And secondly, in a cyber response, you can't just turn your systems on because you don't know whether they're infected. You don't know if by re-enabling them, you're going to, you know, spread the virus further. For example, you really just don't know. It's not a time for panic. It's a time for clear thought and getting yourself organized and for the health sector. The impacts of everything coming to a standstill are huge. One of the first things I got involved in when I started my role was, was to a compass that was a privately owned business, but government funded to a large extent. The chief executive at the time was away and and someone was acting, and she did a marvellous job of trying to manage the response. We got pretty involved because, you know, the government was particularly concerned about patient information, whether it had been exfiltrated. But nonetheless, there was a concern. And, you know, the thing that I would suggest everybody

needs to think about is being ready to respond. This is not something that you can practice, but you should at least be practiced, if that makes sense. So you should at least understand what are the important first few steps that you will take in the event that you find yourself in a situation where you've been advised that date has been taken or potentially taken, or worse still, your systems are down and you can't operate your business and you need to have a plan and you need to be ready to respond. And you just can't build that on the fly. And that's probably the one thing that I would suggest people get ready for. And then I think number two for me would be you need to have advisors. This is not something that you practice that. And there are organizations out there that are they deal with this every day and you should be prepared to take their advice. But whether boards take advice or not is one thing. And we know from media headlines that the fallout can be huge. Optus data breach exposes personal details of nine point five million customers. DHB hit by crippling ransomware. Patient safety incidents are linked to one of the UK's most sensitive data breaches. Millions at risk after justice system fiddles divert ambulances after cyber attacks shut makers over cybersecurity failures. Hackers steal patient data in New Zealand's worst ever health cyber breach. And being brought into the Waikato DHB response as an experience Shane will never forget. My involvement was really, you know, providing national support to, you know, to the district health board at the time. And and at the time, they didn't have a board, they had commissioners. It's time for cool heads. Stay calm. It's a bit scary because you just don't know what you're dealing with. If you talk to the then chief executive at the time, he will certainly be able to share with you what it was like for him. But it was the first, you know, he was the only time he ever wants to go through it because it was massive. When a cyber breach happens, the magnitude is immense and the impacts are far reaching. They had to find a way to get the business running without it. While they worked out how they could get IT systems back up and running. Clearly, there's a lot of media interest. There's a lot of patient interest. You know, there's a lot of anxiety going on. You do think a lot about the people potentially, you know, the information is out there to be seen. And for some people, you know, they don't care. For other people, it's really important because somebody may not want their address details known. You know, they may be living in a, in a relationship or trying to get out of a violent relationship. You know, address unknown, except that somebody leaked their address. And so, you know, there's this whole concern for the patients and the information and the management of their privacy. And then there's the running of the business. In this case, how do you get back and provide health services? And, and so there's an awful lot of, uh, well, while we deal with the cyber response, how do we deal with, in this case, our patients and as an organization technically isolated, everyone decided that there's, you know, we have to disable all the connections. And that meant that, you know, those organizations couldn't necessarily do their job particularly well. And obviously, in this case, the DHB couldn't and they had to organize patients to be seen elsewhere because they had patients turning up that would need support. And they had sufficient, I guess, paper based documentation to at least know a bit about what's going on. But it's pretty intense. It's one of those things you hope never happens to you, but it's best to assume that it may therefore be. Be prepared. It is all go at many levels. How quickly can you get organized? How quickly can you get your head around what's going on? Who is in control? What is the command and control structure that we need to run this by? Are they around? How do we get hold of them? Like it's all go, you know, and the adrenaline is pumping, to be frank. And everyone wants to

know what's going on and when's it going to be fixed. And I don't know yet. And well, the media are nothing and it relies on a whole bunch of trust. I like the term trust and verify, which is asked all the right questions, but be prepared to verify you don't want to reach in and do management's job. You know, the people running the response need to be able to run the response. But but as a board, you need to be confident. It does pay to verify some things as well. And as a board member, you really want to know what's going on. You really want to know truth. You really want to know how should we manage this? You really want to know that people are getting advice and that they are listening. And then to double down on that pressure when the media get wind of the scenario. It adds a whole other layer of stress. The right time to talk is when you've got the information you need, and you can provide something that's coherent and makes sense. There's no point in making it up. You just better say, look, we still don't know. We think then, well, we'll have a guess at it. But at some point you do have to be clear. We now know this. And then what are we doing about it? But for boards, ensuring they're working closely with management and keeping the lines of communication open as key to coming out the other side. From a human nature point of view, people will will like to tell you things. Fine. They'll like to tell you it's not as bad as they think it is. Equally, there is a temptation, and we did see that with one of the more recent responses. We are too quick to tell people that there's an issue. If you can't quantify what's going on, then you need to be prepared to just ask people to wait. You know, there's a whole bunch of things that you just don't want to be doing too soon. And again, at some point you'll get the, you know, the media potentially saying, well, you knew about this, but you didn't tell us. And that's that's right. We didn't because it wasn't appropriate at the time. Part of this is not because you're hiding anything, because you're managing the bad actor. I mean, if you start revealing how they got in, then there's plenty of other people that are going to go and see whether you fix the problem or not. But with any crisis, there needs to be room for error. And that includes understanding that there's a human impact involved. And that not only dictates how people respond in the moment to an attack, but their ability to come out the other end there in the middle of a response. You know, people need to be able to get it wrong. It happens. There's no time to deal with that in terms of why. And you could have done better. Like you just have to accept it and move on. The blame game just doesn't work in the middle of response. Equally, there'll always be some sort of postmortem after an incident, and there'll be things that will be in the category of could do better or could have done better. The most important thing there is to learn from it. Obviously fix the issues and avoid a repeat. You don't want to think hierarchy and go, well, you know, most senior person in the organization or maybe in charge of technology naturally will lead on a response. Some people just don't cope with incident management. You're either a natural or you're not. And I have to tell you, through Covid, what I learnt was a lot of people were very happy to get out of the firing line, and no disrespect to them, but they weren't incident response people. And so you need to know who your incident response team is. And I wouldn't say enjoy it, but I want to be part of it. You have to be an organizer if you're an incident response manager, for example. There are certainly well-trodden paths in terms of how to best manage a response, and that's where those people are experienced and advised, and that will come in. If you're just a business that's providing sort of everyday services. That's one thing. If you're involved in a business, that's health, that's another thing. And there are lots of other businesses and industries where how you manage the response and what you

communicate when is really important. It's, um, not really a runbook, but it sort of is in the sense that you will run through a series of, you know, steps in the process and there'll be decisions you take along the way and communications that you make. And again, that's all part of being practiced and having the right partners when the situation unfolds. Now, Shane can tell you one thing for sure. An incident as big as this lingers long after it takes place. Yeah. Well, it's yeah, as I say, it's it's, it's pretty daunting. And there are people that offer services, you know, and that's part of your cyber response, if there's been a privacy breach, will be providing services to people who need to be helped through pretty tough time depending on, you know, what's going on. So yeah, So you don't want to go through. But if you have to be well dressed. All organizations need to do as much as they can to avoid finding themselves in a situation where they're exposed, but it is all risk at the end of the day. You can spend an enormous amount of money trying to protect yourself against scenarios that are little green men from Mars, you know, may come down and do something, but what's the likelihood? And so you do have to assess risk at a board level and make decisions around where you need to invest. And also, for example, you can have, you know, disaster recovery scenarios that are designed for zero outage failover, like you are so protected, but they're awfully expensive. And then it's which of the systems are the most important and how long can you run as a business without it? Because there's no point in designing for a, you know, almost instant failover to systems When an hour or two or three or a day or a week is actually something that you can live with as a business. So risk becomes a really important factor in decisions you make in terms of where you you invest because it is ultimately unpreventable. You know, my strong advice at the board level is it's very much risk focused rather than spending enormous amounts of money protecting yourselves to the nth degree to hard. That was Shane Hunter. You also heard Susan Cuthbert and courtiers Patrick Sharp, and I'm your host and producer, Sonya Yee. If you'd like to find out more about the Institute of Directors, including how to become a member or for free tools, resources and information about governance courses, head to iodine dot org dot nz. Until next time, Ma. te wa