YS UP GOVERNANCE AND BOARDS PODCAST

Episode 17 – Cyber Part 2 – Data Breach Crisis Communications & Reputation Risk with Karissa Breen

Transcript

Intro:

Welcome to YS Up Governance and Boards podcast brought to you by 3YS Owls Governance Consultants. Covering hot topics in governance, risk. latest regulatory changes and issues keeping directors and executives awake at night. Here are your hosts Ainslie Cunningham and Deb Anderson.

Ainslie Cunningham:

Welcome to another episode of YS Up. Today we're joined by Karissa Breen for the second part in our cybersecurity series to cover communications during a data breach. So, Karissa Breen or KB as she's better known is an entrepreneur, and as an ex techie saw issues with the way the cybersecurity industry was engaging with people. Having worked on the front lines of tech, she founded KBI to help global enterprises frame and develop their engagement strategies. Whether marketing, internal communications or PR. KBI is 100% focused on helping tech companies communicate better with their audiences. Welcome Karissa.

Karissa Breen:

Thank you. Thanks very much for having me Ainslie and Deb really appreciate it.

Deb Anderson:

Thank you.

Ainslie Cunningham:

So, tell us a little bit about your background.

Karissa Breen:

Well, I always love this question because I definitely have a random background. So before we started recording, I think Deb asked me where I was from. So, ultimately, I've been in Sydney 10 years, but I am a Queenslander. I was born there, and family obviously were cane farmers, but I wanted a shift in scenery. So, I moved to Sydney. My career in IT didn't really start up until about seven years ago. And that started when I worked for Commonwealth Bank of Australia. I was working not in security then I was working just in IT in general, but I found a really big interest because I was fascinated as to why people, especially cyber criminals were doing things. And I had a lot of questions around. I was really, really curious. And then I went up to the CSO and I started asking him all of these questions.

Karissa Breen:

And he was like, "Well, no one really at your level asks me the questions that you've been asking." And I think in order to do really well in this industry, you need to be curious and you need to ask questions. And that's when the pivotal moment in my career came, when I moved from being in IT into cybersecurity and my first role there was a reporting analyst and it was probably from that moment. Now it wasn't the genesis of why I created KBI, but I started to understand the

importance of communications because part of my role there was to write board reports, and to talk intelligently around the aspects of cybersecurity and communicate that up to the board. And I started to understand at a fundamental level what the key ingredients were to communicate into that in terms of to people who were not cybersecurity people at all. And then throughout my career I talk on various roles within the bank, and then also moving outside of that into consulting.

Karissa Breen:

And I still used to fall back on always being a communicator and being that voice for super technical people. And one of the things that I find really interesting is that everyone always talks about technical capability, but now in the last five years, we're really talking about the communication side of it and those soft skills, which I think are hard skills and are necessary skills to have in this industry to be able to talk to people about such a complex technical topic. And to be able to communicate that to people in order to get them to understand why cyber security is important, but also to get them to give you money, especially if you're working at the large enterprise level. And so, then I went on to create my own company.

Karissa Breen:

So when you read my bio out and I still think about that time when I jumped ship from working in a company doing my own thing, and running my own firm in three years is because there's been that gap around the technical and in the business. And I wanted to marry those together. So three years on, we do work with start-ups and large enterprises to help them communicate that message. But one of the things that's really interesting that I'm seeing is that lack of communication skills, and lack of understanding when people are communicating data breaches. So when you approached me, I was really excited to talk about this because I don't believe a lot of people have this done well, and I'd like to perhaps shed some light on it today.

Ainslie Cunningham:

Fantastic. So in your experience then KB, how would you find most organisations are doing it and how can they do it better?

Karissa Breen:

Yeah, I think one of the interesting things, when I was reporting is that we would get a bit of a landscape snapshot to provide executives with what was happening out there. I think there's this fallacy that'll never happen to me and it quite often does. And then it's this panic of, "Okay, now it's happened, what do I do next?" And so, then there's that scramble to try to manage it. And then more often than not that I see people don't manage it very well at all. And then as a result of that it becomes bad reputation in the market. People don't really trust you anymore, and it's even harder then to rebuild that trust once you've lost it.

Ainslie Cunningham:

Yeah. I think a lot of businesses overlook brand and reputational damage, and the impact of that and the recovery of that if it's even possible in some instances.

Karissa Breen:

Absolutely. There was a study done recently, or maybe recently a few years ago. It was actually in the United Kingdom, and they had interviewed all these people about if a company would breach were you to go back as a consumer to engage with that company. And I think it was like 70 plus percent of people were like, "No." And so that's incredibly concerning because data breaches are happening left, right and centre simply because we predominantly have companies operate on the internet and that's where it starts. And I think that it's something that people do need to be aware of. But again, I think people are so busy with the day to day and trying to manage even their own cyber practices and then doing the communication side of it. It really does fall by the wayside until it happens. And then they're, again, last minute scrambling on, "Well, what do we have to do now and how do we manage it?"

Deb Anderson:

And communication along the whole journey is important too isn't it. So even you have a breach, even if you're still in the early stages of investigating that breach, it's important to just communicate and say, "Look, this has happened." We're investigating it and we'll just keep you informed along the way.

Karissa Breen:

Yeah, you're absolutely right. And I think a lot of the things is we'll probably get into it a little bit later, but the thing is when you talking about a breach, I think the main thing that I see is people actually communicate too early about what's going on. And I think that's purely because there's a disconnect between the PR, or the corporate affairs manager and the actual technical team because perhaps they don't really know what that means. And so, they've maybe overheard someone and they've misconstrued information. And then all of a sudden, they deploy that into the media, and then the media has got a hold of that. And then all of a sudden, this story has just created this massive impact in terms of people reading it. And then it's just over-exaggerated what's actually happened. And so, I see that a lot because people are ill informed and therefore, they get a hold of something and then they can write a story on it.

Ainslie Cunningham:

So, coming from your background, Karissa, let's talk about how you would go through the process. So, a company has suffered a data breach. What's the first steps they need to take initially.

Karissa Breen:

Look, I think initially now every company varies but if we just use a... In terms of a very broad stroke approach because this could be applied. I think the main thing is having a bit of a triage, meaning identifying who those key people are in the organisation to respond, to communicate and to remediate. I'll be honest with you. Most people can't even get to that stage. So, when it's like, "Cool, we've had a breach." And it's like, "Okay, well then who's on the team to be able to do that." So, most people are still stuck back there in terms of identifying who those key people are. So, once you've done that, it would be in terms of, I would probably look at it as having like six comms streams and I'll get to the reason why that's important. So, it would be management, internal staff, suppliers, customers, external stakeholders, and media.

Karissa Breen:

And so those are the six streams I like to look at it in because your discourse and how you communicate to each of those streams, won't be too much of a difference. But the discourse in which you operate and how you communicate that will be fundamentally a little bit different anyway because they are different types of people that you need to be able to communicate that message. And so, once you've identified the team, you've identified the streams of people that need to be across this. You then need to have some type of comms prepared. A lot of the time, people don't even have basic comms frameworks on if we got breached, do we have something that we can get out to people. Because you do need to notify your customers, especially if you're an Australian business and you're turning over more than $3 million per annum. And it is being classified as a data breach, you have a duty of care to respond to the Australian Information Commissioner on that.

Karissa Breen:

And they will then advise you on what their frameworks are in terms of advising your affected customers. And so once that's been established after that, you need to have a very clear plan on what you intend to do about it. And actually, going to the incident response team that's sitting in your cybersecurity practice to derive what the chain of events and how that actually happened. Because again, as I was saying earlier, it's very easy to communicate the wrong thing. And then all of a sudden, the media has a different story. Then you need to be able to talk intelligently to your internal staff about what the whole company needs to do collectively and cohesively to manage that message. The last thing that you really want to be able to do is that some junior developer has heard about what's been going on and all of a sudden, he's speaking to a journalist and it's really misconstrued the message and it really muddies the water.

Karissa Breen:

And that's something that you want to be able to avoid because it's hard to recover then from an ill-informed message rather than being upfront about what's actually going on. Then once you constructed all of the messaging you need to be able to decide who is the person to communicate that message, especially when it comes to external media. And a lot of the things that I've seen most people, again, don't actually know who that is because it might not be the CEO. Maybe it's the corporate comms lady, maybe it's the incident response guy. And so I think really understanding who that main person is to communicate that, and it needs to stay with that person because it's very easy then to chop and change. And all of a sudden there's Chinese whispers about what's actually happened. And then again, that's following the plan that you've put in place. How often should we be communicating? What channels should we be communicating? What type of information should we be communicating? And so, then you'll obviously need to rinse and repeat that process until there is some type of resolution.

Ainslie Cunningham:

So. for businesses who might only be maybe that three mill mark, they do get caught up in the legislation requirements for divulging, if there's a data breach has happened. But they might not be of the size to actually warrant a position for a full-time person, a chief security officer, a chief information officer, a PR team, or anything like that. So, what are the sorts of things that a business of that size need to do? You've touched on some of those points about having crisis comms drafted and things like that already. What are the other things that they can do to manage any impact to brand or reputation damage?

Karissa Breen:

Look, I think that's a really good question. And I think that is such a common thing that we do sort of see as well because these companies they don't have enough budget to hire a whole fully fledged team. But I think first and foremost, you need to have some form of immediate statement ready to go straight off the bat. It doesn't even matter if you think that it will never happen, chances are it may and it's about being future proof that if it were to happen, do you have something ready to go then and there. At that type of situation, time is so critical that every hour that ticks by and you haven't responded because you don't know who the person is to respond, or you don't have anything in place. And you're trying to sort of engage with an external PR agency or whatever that may be, have something ready to go just in case because at least you've thought about it because a lot of companies even at the large size don't even think about this either.

Karissa Breen:

And you coming in more of an offensive approach. And what I mean by that is instead of sitting there acting defensively when media and all that type of stuff are coming to you, you can say, "Cool, this is the state of affairs. This is what happened. And this is what we are doing as an organisation to remediate the issue to really rectify it.

Deb Anderson:

Do the OAIC have good resources on their website to help companies when they have a data breach?

Karissa Breen:

Sorry Deb I just lost you there, what did you say, sorry?

Deb Anderson:

Sorry. Do the OAIC have good resources on their website to help if you have a data breach incident?

Karissa Breen:

Yeah, absolutely. Absolutely. I think one of the bit of feedback that I do hear is that sometimes it can be too detailed and people, when they look at it, they just feel really apprehensive about reading a 60 page document on how to go about it. So that would probably be the only thing that I have heard when people are looking at government websites, that they feel overwhelmed by the

information out there. And then as a result of that, they're like, "It's too much. I couldn't be bothered sifting through this information."

Ainslie Cunningham:

Yeah. Absolutely, information overload isn't it. So in terms of establishing a core data breach response team, who are the key players. You've mentioned previously the CEO and maybe a PR person, but is it worthwhile getting in an external PR agency in this space?

Karissa Breen:

My thoughts around that would be, there's this common failure that I see in the industry as maybe what I touched on earlier is you've got a PR agency. They don't really at a core level understand cybersecurity. And so then there's this gap and that's how I created KBI because there's this gap. And as I said too, as I mentioned earlier, that people are out there communicating the wrong thing. So, I'll give you an example. When COVID happened, everyone went on this government website, all of a sudden, it's gone down and a government representative came out front and centre and said that they had been DDoS'd (Distributed Denial-of-Service Attack). Now that's actually not what had happened. So, he got his facts wrong. And then all of a sudden, they had to write another statement around what happened in that event.

Karissa Breen:

And I think that because PR agencies haven't worked in cybersecurity and it's very nuance and the language is very particular about what certain elements mean. It becomes hard for them to understand at that fundamental level, what that actually means. So, you could do that. I would say having a comms person embedded in your incident response team. So in your SOC security operations centre for that person to work with the super technical guys to understand what's going on, and then to relay that to the business then internally to say, "Hey, this is actually what all these technical jargon and means in layman's terms."

Ainslie Cunningham:

So, when you're communicating with boards and management teams, how do you manage that communication conduit, so that you're breaking it down in an element that they understand?

Karissa Breen:

I really love this question because I think that that's the operative question that everyone keeps asking in this industry. And I think for me personally, how I see a board member, I've been doing this for a number of years is they're just human beings as well. And they have the same interests that perhaps you and I have, or they have common ground. And I think that using analogies that then are relevant to those people then as well, and not speaking so abstractly about a situation and really bringing it down and bringing it back to basic, and not being so esoteric around the language that is used. And I think that it's about understanding your board members and what they actually like, and then try to use examples and analogies that make sense to them. So, if they love surfing on the weekends, then talk more intelligently about that and try to relate it back to them because people relate to people at the end of the day.

Karissa Breen:

These people really are just human beings. And I think that the reasoning why this industry has not quite gotten that is because they're not people's people. They don't understand human beings and I think that when people were taking Comp Sci. degrees back in the day, they thought, "Well, I'm going to do this degree because I don't have to deal with the humans because I don't particularly like them. Well, I feel socially awkward around them." And I think what's come full circle now is I had a professor on my podcast recently and she's like, "It really gets to me that a lot of these students don't know how to communicate. They can't write presentations. They don't know how to speak to clients. They can't communicate at an executive level." It's because they're not teaching it back in university or colleges. And then all of a sudden, they've gone throughout their career.

Karissa Breen:

And IT traditionally operated as an independent silo just on the side. But now IT is the backbone of most organisations these days. Most companies are tech companies and being integrated, and now they don't know how to communicate. And so, what we've had to do as an industry is almost retrofit, "Hey, this is how you talk to people. This is how you influence people." And most people at that senior level who are in cybersecurity are not leaders, they just got in there by default. And so, then if you pull a leader in from another part of the business, they don't get the security side, so again, there's this massive disconnect that were seeing. And no one seems to be able to look at it holistically, like actually you do need to have some technical understanding, but the key thing here is to be able to communicate and influence people.

Karissa Breen:

And I think if we had been better at that fundamentally, we would be further along, but unfortunately, we're not. And the average calibre of people that go in IT, don't like human beings. So hopefully, in time that will change.

Ainslie Cunningham:

So how do we bridge the gap?

Karissa Breen:

Sorry.

Ainslie Cunningham:

How do we bridge that gap?

Karissa Breen:

In terms of getting IT people to like human beings, or?

Deb Anderson:

Robots.

Ainslie Cunningham:

Just communication really. How are we really going to try and bridge the gap between IT teams, senior leadership teams, executives, especially pre-planning for a data breach, like you say, or worst case scenario, a data breach has now occurred. And some of these organisations have not been well prepared. And how do we really bridge that gap.

Karissa Breen:

In terms of the bridging the gap it's about hiring people from different backgrounds, people from comms backgrounds that they can teach the technical side of it. And you don't have to be super technical to understand it at that level. Since I've been doing that, my skill 100% had probably atrophied on that level, but I think it's about understanding from an executive point of view and saying, "This is really, really important to us as an organisation." And then that executive needs to be able to feed that down through the chain because if they're not chanting it at the exec level at the CEO level, then no one else really cares. It's got nothing really to do with them. And I think that that's definitely been the problem that we've seen, or I've seen, especially working in a bank if people at that level don't endorse it, it just sort of falls by the wayside.

Deb Anderson:

I think one of the main challenges, there's quite a few challenges, but one of the main ones is you have a data breach is communicating effectively with your customers, your clients, as to what's happened and to have the right people on the other end of the phone, fielding those calls and having those discussions, what are your tips in doing that really effectively.

Karissa Breen:

So, as I mentioned before, having that cohesive message, so you don't want for the message to be diluted or disparate that the executive guy is saying one thing, and then the other guy the developer saying another thing. I think, for example, it would be forming that team. And then distilling that message down into what does this actually mean for people who are not from a technical background and putting it in language that they can understand. And then again, having that centralised person or that team or that call centre that takes those calls. Because once you start then chopping and changing the message, people get really, really confused. They get angry on Twitter, they can get really that they feel left out.

Karissa Breen:

And one of the things that's really important is that no one gets in trouble for having too much communication. Where companies fall down is if people haven't communicated enough about the process. So, people might feel like they're annoying people, but people genuinely do want to know what's going on first. Well, they were breached and then nothing was said, for example, Equifax, that happened. And that was the worst approach you can do is say nothing.

Ainslie Cunningham:

So, I guess where companies do have that in house team or they've appointed an external PR agency to manage consistent messaging. They've got people fielding calls on the other end of the phone of angry customers who's potentially, their information's now out there in the ether and potentially exposing them to risk. What are the things that businesses can do to manage the impact to their brand damage?

Karissa Breen:

Oh yeah, that's a really good statement because as we were mentioning before, once that's done, it is really hard to repair. I think that one that's just going to take time. That's definitely not going to happen overnight. And I think, again, it's about talking through from a communications perspective about what their company's going to do long term at each stage gate around what that actually looks at. And I think the other thing as well is media train your executives. That was something I was going to mention earlier. It's because I've sat on panels, alongside people from large corporations that aren't really good at communicating. And I think that if these people who are on the frontline around giving this message, or perhaps trying to instil trust, these people definitely need to have training because journalists are employed to do their job at getting that message.

Karissa Breen:

And they can ask questions in a way, which almost gets you to shoot yourself in the foot because of how they position themselves. And I think there was a really good interview that Jordan Peterson a journalist, and she kept putting words in his mouth and how he recovered from that was really, really interesting. And that's something I haven't seen a lot of in Australia, in the US their executives are a little bit more well versed at media training. But definitely in Australia, they need to be, because again, you need to be the person at the coalface providing the comms, but also trying to bring back that trust then over time. And I would say that that's going to take time, but again, it's going to be having a level of integrity. So, do as you say that you're going to be able to do.

Deb Anderson:

I think it's about being empathetic too, isn't it?

Karissa Breen:

No, you're absolutely right. And I think the other thing it is as well is don't try to cover up what had happened. I think just owning it and saying, "This is what happened. However, this is what we're going to do as an organisation to remediate that." And I think one of the things that I found interesting was Barack Obama got asked in an interview like, "Hey, were you smoking weed?" And he just owned it. He doesn't have anything to hide then after. If you're saying, "No, that didn't happen." And you're trying to position something else, you get really defensive. And it's obvious then when you're lying. And I think that once it's out in the open all you can do is go up from there.

But if you're trying to be very invasive about it, it actually can do more damage. Because again, it's coming back to that integrity piece.

Ainslie Cunningham:

In terms of some of the other things that you have seen businesses do in this regard. Some of the banks they might offer a token credit to people's accounts or other businesses might offer gift voucher, or something like that to soften the blow. Where there's been businesses that have kind of tried to win back the trust, they've regained their customers, and then it's gone and happened again. We've seen some really large organisations in Australia have repeat offenses in this space. What's the recovery look like for those brands?

Karissa Breen:

Yeah. I think again, Australia is a very trusting nation. So, when household brand names, this does happen again, it's really, really hard to be able to recover from that. Again, it's probably going to come down to the CEO running this at the coalface around having that level... I don't want to keep going back to it, but yes, having that level of integrity, but again, being very open about what's happened and having a plan in place. Saying nothing or not communicating the facts is the worst thing. And I think that there's no real, this is the way to do it because it would depend on each individual scenario. But as I said, not enough people are just being honest about the situation and saying, "We really care about you guys and having more chains of communication. I think even at the moment, with everything that's going on with Twitter. They've got a dedicated support page so people can get upset, but they are responding to people quickly because people hate to feel that they aren't heard.

Karissa Breen:

And I think that when you're dealing with a breach or an incident, you need to be really quick to be able to respond to these people. So, they feel heard and generally, if you continuously try to do that, and you are putting mechanisms in place to better the brand over time that should soften the blow. But again, once the damage is done it is really hard, but you need to be able to future proof perhaps what that's going to look like. And actually, while thinking of it, Red Cross, how they managed their breach. They still wanted to engender trust. So, people continued to donate blood and that's exactly what had happened. So, I think that was a really good way to look at it then as well, in terms of a way that companies have managed breaches effectively.

Karissa Breen:

And Norsk Hydro was an aluminum company. They had a massive breach but how they communicated and handled it, their share price went up. So again, those are rare, but there are good test cases out there around how a company has managed it effectively and that have come full circle. And I think people are forgiving in the sense of, "Okay. Yes, they stuffed up." But they've being really proactive in their approach, their comms and their level of integrity to be able to manage that moving forward.

Deb Anderson:

So, with the threshold for a reportable breach. It still doesn't really take away from businesses of all sizes. They still can have a data breach. It's really the same systems and processes in place. You're just not reporting to the OAIC correct?

Karissa Breen:

Yeah, that would depend. So, in terms of regulated industries, so like fin services and health, there definitely are more regulation around that. And I think that's a good thing simply because people's backs are against the wall and they feel well, I've got to be compliant. And that gets them to think about security, but other industries that are not heavily regulated, not necessarily. And so that then becomes the downfall because they're not being monitored. It means that perhaps they're not considering security because nothing's necessarily going to happen. They're not going to lose their license or anything like that. So, to some degree, that's why I like regulation and compliance for those reasons.

Karissa Breen:

And I think over time, they'll try to span across more industries that I've been speaking to people on my own podcast. But again, it's just going to take time because when you think about the internet, like when you have a driver's licence, it's like you have rules and regulations that you abide by. But on the internet, it doesn't really work like that. And I think the cybersecurity industry is constantly just trying to play catch up with what's going on. So when you talk about a future proofing, having comms, it just feels overwhelming to a lot of people.

Ainslie Cunningham:

So, you talked briefly before about having those six different silos and different types of messaging. Can you give us an example of an internal communication versus an external communication, and what sort of messaging you would be giving to staff as your internal stakeholders?

Karissa Breen:

I think where an internal, and that's going to be dependent on how you... You do want to be honest, but then you don't want to be so honest in the fact that some guy goes home and tells his wife, and his wife knows a journalist at the media company, for example. So, I think just being very clear and concise and being honest about what happened, and what the organisation's going to do about that and what that individual then needs to do. Like what's their participation in it. So, it could be, if you get phoned up by is a journalist, don't answer that call and just say, "Look, I'm not the right person to speak to. But Sally, who's the corporate comms manager, she can funnel your call, or we do have our hotline number that you can call up in terms of understanding a little bit more about what that actually means."

Karissa Breen:

And so in terms of the media side of things, that is always a very interesting one because sometimes it doesn't really matter what you say, that they'll misconstrue the information and then start writing a headline about something. But again, it's about being honest. You can't be evasive about the situation and then saying, "Hey, we do have a plan, and this is what we intend to do about it." And being very short and concise, you don't have to be super detailed. And I think just doing daily updates on your social media accounts around this is what we're doing. And if you have further concerns, "Please call this number and our team who have been trained internally to be able to respond effectively."

Ainslie Cunningham:

And how do you manage that? The lag time between one identifying that a breach may have occurred and to the point where we've now got a handle on that information, and we understand how people have been impacted, what information may have been leaked, etc. Sometimes there's quite a lengthy delay between those two points because it can take some time to identify and track where information may have potentially been leaked.

Karissa Breen:

Yeah, you're absolutely right. There are statistics that some companies won't even know that they've been breached until 200 days or something ridiculous. So, it is really, really hard to tell, but I think that as soon as you know something, you need to be able to have that triage meeting. Bring in the appropriate people to say, "Okay, what's going on? And how are we going to be able to manage this?" And I think what companies should start to do is have that playbook in place, have some type of framework in place about what actually happens. And I think Ainslie how you and I met originally was on that BCP webinar.

Karissa Breen:

And that was really interesting because the same type of concepts still apply to this. And knowing, "Well, what do we do now?" And I still don't think a lot of people have really nailed this. But I think that again, having some type of communication straight off the bat to be able to send out to people is what you need to be able to do. Again, it doesn't need to be an essay. It just needs to be, "This is the thing that's happened. This is what we're going to be able to do about it." And have that bullet pointed or one, two, three around this is what we're going to be able to do.

Karissa Breen:

And then when they're going to be able to hear more communications from you. So, if it's daily, make sure it's daily, don't say daily, and then it's weekly. Again, that will then lose trust in people because you're not doing as you say you're going to be doing.

Deb Anderson:

So, have you got any statistics about generally how long the whole process takes from the time of the-

Karissa Breen:

No, there must've been a lag there, sorry. Sorry, Deb I must have cut you off.

Deb Anderson:

No, it's all right you go.

Karissa Breen:

Not specifically, again, it's going to really depend on the industries if they are regulated that could be longer because they have to go through their whole process. They have to audit what's going on. But no, I don't have any statistics on hand, unfortunately.

Ainslie Cunningham:

Before we wrap up today, Karissa, is there some top three tips that you'd like to leave businesses within terms of your skill set and the benefit of hindsight in some of these scenarios?

Karissa Breen:

I think having a playbook, so having some type of basic framework around if something were to happen, do you have comms that you can send out then and there? I think if it does happen, be honest, don't try to cover it up. Don't try to lie about it. Be real about the situation. And then number three, really identify who those people are in the organisation. And then start to test or war game the situation as well. I don't think I touched on that, but again, when these things happen, and people feel really stressed and they feel overwhelmed and they don't know how to manage it. So, I would say probably every six months go through, if we were to be breached, how would we as an organisation manage this? Because last thing that you really want to be able to do is know that you don't have that confidence in your staff to be able to respond effectively.

Deb Anderson:

Great tips.

Ainslie Cunningham:

Yes, absolutely. Get your war game on.

Karissa Breen:

Thank you really appreciate you guys having me today.

Ainslie Cunningham:

No worries. Thank you so much to all our listeners for joining in today and thank you so much Karissa for joining us.

Karissa Breen:

Thank you so much for having me. I really appreciate it.

Outro:

That's all for today. Until next time, happy podcasting. And remember if you're enjoying the show, check out our other episodes and all things governance at www.3ysowls.com.au.