Speaker 1: Hello and welcome to the CPA Australia podcast, your weekly source for business, leadership, and public practice accounting information.

Drew Fenton: Welcome to the CPA Australia and Pitcher Partners podcast series for the not-for-profit sector. In this five-part series, we discuss some key issues for those working in the not-for-profit space, covering a different topic each podcast. Today's topic is the third in the series, cyber security. My name is Drew Fenton, and I'll be hosting today's podcast.

Drew Fenton: A little bit about me, I'm an experienced director with a demonstrated history of working in the insurance industry, skilled in professional liability, risk management, property and casualty insurance, excess and business development. I've been a CPA for over two decades and have published in magazines such as "*In The Black*," which will be put up as part of this podcast. With me today to talk about cybersecurityis our presenter, Krist Davood.

Krist Davood: Thank you. My name is Krist Davood, I'll tell you a little bit about myself. I'm American-Australian, so pardon the accent. I have been in Australia for a few decades, but the accent isn't totally gone. Started off in the technology industry going back 28 years ago. The early part of my career has been quite tech-y orientated around technologies, both from an infrastructural network perspective as well as software. The middle part of my career has been spent around doing more multi-national type implementation work, and obviously a big part of that is security, which we'll get into shortly. And the latter part of my career has been more executive level focus, so more around myself being an executive, but as well as serving on the boards of three not-for-profit organisations.

Krist Davood: My role at Pitcher Partners, where I've been for the past three years or so, has been at the principal level there, hitting up the cybersecuritypart of Pitcher Partners. In regards to qualifications, my highest qualification is a masters in information system management from Swinburne University. The type of work that I do now is really across Australia, obviously, supporting organisations around cyber security, but also assisting and to do something about it, hence my project management and programme management background.

Drew Fenton: Krist, we hear a lot about cybersecurity. How real is the threat of cybersecurity for not-for-profits?

Krist Davood: The threat is very real, and let me back up that statement by just stating some facts. So, the first fact is that the situation has gotten so, I suppose, urgent that as of February 22nd of this year, being 2018, a new scheme has been put into place, the notifiable data breaches scheme, NDB, specifically mandating that organisations not only notify the authorities within the government, but also relevant stakeholders. Customers, staff, and other relevant stakeholders as well, of any data breaches, which could be technology based or it could be paper based, meaning people walking out of your organisation with sensitive

information. So, the answer to your question is that it's very real, just going by that fact alone.

Krist Davood: The second fact is that it seems now that every week that we hear about new breaches, not just within the not-for-profit sector, but also in other sectors as well. Now, as more and more people cotton on to, I suppose, various organisations' weaknesses, and I'm talking specifically about not-for-profits now, will be put in a situation where we really need to think more about the security posture and risk posture of not-for-profits, particularly when I consider for example, donations, for example, to not-for-profits. We have a channel through to the public domain for people to give us our funding, so to speak, to provide a donation. By that alone, you're opening up the door to potential hacks. So that's one example of a potentially growing weakness.

Krist Davood: Other facts are that you're seeing the emergence of something people refer to as the dark web, which is, for those of you not familiar with the term, is you could say a digital black market, if you will, to trade people's information. And in this domain, relevant information that is on offer to not-for-profits, for example, credit card details or personal address or residential details, are up for offer. So the answer to the question is that it is real, and there's a number of facts that support that conclusion.

Drew Fenton: Thanks, Krist. Could I say, from an insurance perspective and a risk perspective, we would always encourage our clients to, as best they can, assess their risk profile and then obviously take appropriate measures on the other side of that risk profile, whether one deems it to be high, medium, or low. Now, the next one, Krist. How will we know when there has been a breach?

Krist Davood: So the first one is when there's unauthorised access to data. The second one is when there's accidental or intentional disclosure of information that should not have been disclosed. And the third one is when information is lost. So from that perspective, that's the regulatory emphasis on when there is a breach. Now, when you would know when you have had a breach, some of the circumstances it'll be more obvious, so for example, when hackers come in and they steal data, for example, and they put you up for ransom for stealing that data. That's an obvious case of when data is breached.

Krist Davood: Other instances when you would know data is breached is you may not know for several months, but then all of a sudden, your customers' data is on offer in the aforementioned dark web that I was referring to earlier. So it's not clear-cut when there is a breach, but what is obvious is that at the earliest opportunity when you are aware that there is a breach, you will need to inform the authorities, specifically the OAIC, as to when that data breach has occurred.

Drew Fenton: Krist, thanks. Yes, this new privacy legislation that's introduced earlier this year certainly has put a greater onus on organisations to understand what a breach is and the ramifications thereof. Krist, where should we start to look at cyber security?

Krist Davood: Well, again from a regulatory perspective, the relevant areas that are relevant to not-for-profits, both CPA members as well as the directors and executives that they serve, there's a few key areas to really look at. One area is around governance, as in what level of governance the organisation has around controlling how data is handled and also managing that control as well. Specifically, it's about understanding what level of protection that you do have and how to fortify your protection, particularly from a data perspective.

Krist Davood: The second area is around the policies that an organisation has. So, many organisations have some basic policies in place, like for example, what to do or not to do from e-mail point of view, or from a internet browsing perspective. But they don't have more comprehensive policies around how to manage data, how and when to access information. So from that perspective, policies become quite important and I would encourage CPA members to discuss this with relevant personnel in your organisation. But a policy is a statement of intent from a director and executive's point of view, meaning that it is a document or documents that could be offered up in court or to the OAIC in the instance where a breach has occurred.

Krist Davood: Why is that important? It's because it's a statement as to what these directors, what their statement of intent was, and also articulates their so-called duty of care. What their feel, and what their thoughts are in regards to data privacy.

Krist Davood: The third area is around what the OAIC refers to as data breach plans. But I would offer up the comment to say it should really be a crisis management plan, i.e. you should articulate in very specific terms what to do in the event of a cyber attack. So, it articulates who, what, where, how, and why things need to happen. Who do you need to tell? What do you need to do? Who do you need to disclose the fact that you've been breached through to? How to articulate how you know there's a cyber attack, and how you're going to go about rectifying the situation. So that's a big part of the crisis management plan. There's a lot more to it than just simply that. One example I mentioned before was around disclosure. So, in a crisis management plan, you would have a process, referred to as disclosure protocols, where it has three types of scenarios.

Krist Davood: So the first scenario is, okay, we've had a breach but we're on top of it and here's what you as our customers, or the OAIC, or stakeholders, need to know about the breach. So, in other words, let's say hypothetically from a not-for-profit point of view, credit card information was stolen. In the event of a data breach, it's saying, okay, the breach has occurred. Credit card information was stolen. We recommend, for example, that you replace your cards.

Krist Davood: The second example of a disclosure protocol is around the, well, things are not quite there yet, but let's communicate to our stakeholders that we're slowly getting on top of it and we'll give them an update within a particular given period of time. That's a situation where you're not quite on top of it, but you're nearly there.

Krist Davood: The third template, if you will, of a disclosure protocol is, things are going badly. I mean, you wouldn't say that, but you need a preconceived template or document that says, all right, well, things that are going badly. Yes, we're doing our uttermost best to rectify the situation, but we're not there yet. And what's helpful in those situations is to state the facts. When the said breach occurred, what you're doing about it to try to get on top of the situation, so just articulate relevant facts and some things to give people some sort of sense of your ... There's a lot of work happening out in the background. Those things are helpful to do in advance.

Krist Davood: And my fourth and final point is about really technical controls and how you would manage an incident as it's unfolding. So there's a best practise framework referred to as CREST, which by the way will be in the show notes. But the CREST methodology talks about how to handle an incident. It's my way of ascertaining, it's part of the framework that I use with organisations, how they will handle an incident, what needs to happen before an incident occurs, how you identify where it's coming from, what you're doing in the midst of it, how do you gain control of the situation, and what do you do as a reflective measure to ascertain what happened and what you can do better. Those are things that the government will be looking for.

Drew Fenton: Thanks, Krist. If from an insurance perspective, we look at this, we always think the partners are imperative in being a successful organisation. Not-for-profits invariably have limited resources in a lot of circumstances. Insurance may be an option there to provide additional resources in relation to managing such an incident. For example, cyber insurance, invariably the first notification goes to a solicitor, who understands the legislation and effectively can introduce a way of managing the claim, if the organisation doesn't have such a plan in place. And then a number of experts in relation to IT flowing down through to possibly payment of ransom, et cetera, et cetera. So my suggestion there is, within your risk management framework, insurance may be an option to be considered in relation to assisting the organisation.

Drew Fenton: Krist, what kind of measures do we need to put in place?

Krist Davood: The measures include a lot of the aspects in the previous question around the crisis management plan, which we've discussed, the disclosure protocols, I gave three examples in the previous question. Technical controls become important in that there's software controls, if you will, that allow or disallow access to key bits of information. As well as a proper governance being put into place. But, that all said, let's take a more holistic view of a not-for-profit. When you are on the board, there's some key questions that would need to be taken into account, particularly from a director's or board member's point of view, which CPA members either serve or are one.

Krist Davood: So one of the initial questions is, where is the organization's data? Because the answer to that question allow you to articulate well, where should I put my strongest controls? Your crown jewels, so to speak. Who owns that data? So if

you are in one office, like for example, during my days at [inaudible], which is one of the not-for-profits that I referred to before, it's a disability services and response services based organisation. We had, at that time, four locations. Now it's a little bit bigger. But in that particular instance, there was many owners of data relating to donorships, relating to staff, relating to how disability service related projects work. So that ownership then becomes important because you would want to make sure that there's controls around that data.

Krist Davood: And then, the last part of that question is, and how important is it to the business? It's well and good to say, well, all that information's important. But what's really important? Well, particularly from a CPA and from a regulatory perspective, things like financial information is up there. Why? Because that is what's most attractive to cyber criminals. So you know, just yesterday, and this podcast is recorded as of the end of July, just in the last week of July, a report came out of a full quarter, calendar quarter, worth of cyber attacks. And the top two areas that were attacked is health related information and financial related information. Those are the golden jewels that are traded on the dark web that I mentioned up before.

Krist Davood: So, when ascertaining how important is the data, it's not just an internal question, but it's also question more likely to be traded in the so-called dark web. So when I'm looking at it from a not-for-profit member perspective, I'm also thinking about well, financial information is going to be pretty attractive. Credit card information, BSB numbers, account numbers, other bits of information. Again, I was in disability, it's about health related information. The health information we collected was not just about the people with the disability, but it was also about the mental health of the families taking care of those people. So that information is pretty valuable. So from that point of view, it's not just an internal examination of what's important, but also an external analysis of what's important as well.

Krist Davood: While we're on the topic of looking holistically across a not-for-profit, I would also offer the point that risk management around cybersecurity is not just an IT related issue. It's widely recognised now, it is an enterprise one. For those members that question whether what I'm saying is true or not, if you look at the notifiable data breaches scheme, it specifically penalises organisations, and this includes not-for-profits as well, for those of you that are above 3 million in turnover. But it will penalise an organisation up to $2.1 million. That's a lot of money. And also, individual directors as well, for $420k, individually. Each director. So, from that perspective, there's a lot at stake here. It's not just an IT issue, it's an enterprise-wide issue.

Krist Davood: So in my [inaudible] days, we would be sitting around a table during our board meetings and we would just not only knock things out, but also try to pragmatically understand, how can we control this stuff. And it is possible, so from a not-for-profit point of view, it's not big bucks or dollars to rectify these points, there's some pragmatic solutions out there.

Drew Fenton: Thanks, Krist. Just moving on, to manage our risks, do we need expensive technology or people to do this?

Krist Davood: No, you do not. From a regulatory point of view, the key term here is around reasonable, right? Not-for-profits, they obviously don't have the funding of a bank or a good insurance company, or of any large type organisation. So, [inaudible], if I could use that old expression, meaning that one size doesn't fit all when we're talking about cyber security, or let's just call it data security. There are pragmatic solutions.

Krist Davood: So allow me to give you all some free advice, so to speak. At [inaudible], when we wanted to capture whether directors were on top of cybersecurityrelated issues, and that were tracking our discussion of cybersecurityconcepts, what we did was we captured our notes and our dashboard in an e-mail. We regarded as an official record of our board meeting, and we sent it around via e-mail, so this is in Outlook or a Gmail type service. And now you have your auditable record, that directors have not only had their view and control as to what's happening, but they also understand what the risk exposure is. And now it's an auditable piece of record. So from a CPA point of view, that's very relevant.

Krist Davood: Also, when we're talking about technology, things like anti-virus on your individual computers and on your servers is a very good investment, because you're creating several degrees of separation between you and the hacker, meaning that the hacker has to bust in through a lot more things. And also, lastly as well, is putting in things like, for example, firewalls. Which is a third level of security that could be applied. So now you've got three degrees of separation between yourself and a potential hacker.

Krist Davood: Now, that all said, software or antiviral software is no good if it's not updated. So obviously, always update your software, on servers, on computers, and firewalls. Make sure that any equipment that touches the internet is adequately protected. By the way, for those of you that have wondered the difference between IT security and cyber security, one very simple definition is that IT security, that term was created back in the day where systems were stand-alone. You come into a company, you're not connected to anything called an internet. You have your little system there, you're typing away, doing your work, and that system needs to be protected. Hence the term, IT security, meaning that bit of system is protected.

Krist Davood: Now, we have multiple channels, or some people call them vectors, multiple ways that people can hack into you through the internet, through your mobile devices, through many channels. So going back to the premise of what technology needs to be put into place, just keep the golden rule of anything touching the internet, that piece of equipment needs to be protected. And yes, with the most current of software.

Drew Fenton: Krist, thanks for that advice. This one's always difficult. If we do take the message as you've just suggested, how do we know they are working for us?

Krist Davood: One service that's very widely offered is something that's called penetration testing. Now, the ethos behind the penetration testing is that an ethical hacker would be hired to purposefully try to break into your systems. Now, subject to how good they are, they could go to quite extreme lengths to try to steal your information. And keeping in mind that, I know today's topic is cybersecurity, implying that data could just be stolen electronically, but I would also, from a CPA and not-for-profit point of view, also remind everyone that data theft can occur just by someone stealing a piece of paper. So let's not limit this discussion just to digital theft. But a penetration test, a particularly really good one, would be an organisation who, through a number of mediums and channels, will try to steal your information. So everything by trying to hack into your website through to trying to access your systems, either through the internet or posing as a customer coming into your organisation and wanting to make a donation, for example, through to a person impersonating a telecommunications service person. And yes, these are real examples as well.

Krist Davood: So penetration testing can take many forms and can occur through many different avenues. But to answer the question, penetration testing is one of the best ways of measuring the level of protection that you have. Why? Because it's mimicking a real-life attack. And you also get the results as well. The second part of this answer is also a relatively new process where, on purpose, e-mails are sent through an organisation that are purposefully created to lure you into providing private information. So some IT departments within organisations send out a bogus e-mail, supposedly from your financial institution, to just give an example, asking you to fill in your private information including BSPB account numbers and credit card details. So from that point of view, many of these type of tests, whether it's through that e-mail process that I just described or that penetration test process that I described earlier in my answer, those are two fairly good ways of ascertaining the level of security you have.

Drew Fenton: Thanks, Krist. That was an excellent answer. Going forward, how do we monitor and report on our cyber security?

Krist Davood: From a OAIC perspective, and from the NDB schemes perspective, the reporting process as indicated on the OAIC website, indicates some protocols you need to follow in how you report on cyber security, particularly around when your information's inadvertently accessed or distributed or lost. So it has some key points that you need to fill in. Who's been impacted, why has it happened, how did it happen, where did it happen? So where, it's dependent on whether that's a relevant point. And what are you doing about it and how can you ensure this is not going to happen again?

Krist Davood: There's far more questions than that, but part of my role is supporting organisations and detailing exactly what they do put in such a report, as well as how to manage their various stakeholders. So everyone from irate customers and what you need to let them know so that they don't pursue legal action against you, but also through to other stakeholders as well, for example, staff. So there are protocols you need to follow through, and the OAIC will be

monitoring the situation closely, by the way, hence the changes to the privacy act in February 22nd of 2018.

Krist Davood: Going back to the first part of the question about monitoring, well, monitoring is something that either your IT department or for most not-for-profits, they don't have a dedicated IT department, they have what is referred to as IT manage service provider. Those manage service providers should give a one-page summary on a monthly basis as to what your security profile is, i.e., are your security software, are they all kept up to date. That's one aspect that they need to let you know, and have it as a dashboard. Green, yellow, red, depending on what situation you're at.

Krist Davood: The second point is that is the software deployed in every part of your network? So before that I gave the example, every bit of your network that touches the internet, that should be protected with the software that I'm referring to. But also working back from that, also other bits of equipment within your organisation also needs to be protected as well. And that needs to be part of the report that your manage service provider gives you. It needs to be captured and reviewed by the directors within your organisation, or for CPA members that serve not-for-profits, to your client's organisations. And it needs to be recorded as something that's been discussed, particularly from a director and/or senior manager level within the not-for-profit.

Drew Fenton: Krist, thank you. The question is often raised, what should we tell our clients/members about how safe their data is?

Krist Davood: The advice that I give my clients is, when in the midst of an event, or prior to an event, so indicating how safe their data is, is always to state facts. It is inappropriate and unprofessional to state that an organisation's data is absolutely safe. There simply is no such thing. When you consider that you could walk out with a piece of paper, a USB, you can take pictures of a screen with confidential information on it, through to infiltrating systems, to collecting print-outs, the list goes on and on and on. So it's inappropriate to say that data is safe. You can't say that with 100% certainty. What you can say is stating facts, meaning that we're doing everything as a not-for-profit organisation, reasonably speaking, to protect our data. And here's what those processes are, for example, we're keeping our software up to date. We have monthly meetings on this. Our policies are up to date. Our crisis management plan is updated. We have penetration tests regularly, just to keep ourselves ready for such an event.

Krist Davood: So you could only state facts, and being specific about those facts as well. So saying, for example, "All 17 staff members, their computers are protected," and "We give regular training to our staff members," and "The last one we made was four months ago as of this date." So those specifics and those facts goes a long way to providing assurance, but also to communicating to people, "This is a new world. Data will not always be safe." But what you can do is what you can reasonably do to protect the data. That's all that you can state from a factual point of view.

Drew Fenton: Thank you, Krist. Now look, we will just wrap this session up today. I'll firstly hand out to Krist for his views.

Krist Davood: So on the subject of cyber security, the best thing that CPA members can do for not-for-profits is really to look at this from a regulatory point of view, particularly that understanding the questions that we mentioned before about where is your organization's data, who owns it, how important is it to the business? That gives you a feel for where to invest and to prioritise your efforts around cybersecurity, whether it's on a IT system, or whether it's on pieces of paper with quite detailed and sensitive IP on it.

Krist Davood: The second point is very much based on what I mentioned before about treating it as an enterprise-wide risk management issue. It's not just an IT issue, that's why the government changed the legislation to, for the lack of a better term, force directors and executives to look at this as something that infringes on the privacy of customers and staff members, et cetera. So it is viewed as an enterprise-wide point. So even though that a number of you today may have commented the subject thinking that this is going to be a technology orientated discussion, in fact it is a risk management, enterprise-wide risk management related challenge.

Krist Davood: I thank you all for your time and it's so great spending time with yourselves today.

Drew Fenton: Thank you, Krist. Could I just finish off and just say that we do live in a neat little world and we're all connected. If I look at this purely from an insurance perspective, the real issue we have with this risk profile is that the risk is changing on a daily basis. We have a number of regions in the world which are developing new ways to hack your system. The virus that was introduced last week is now not relevant the next week. So as Krist mentioned, the most important thing here is to understand your risk profile and put in a solid methodology in relation to managing your risk going forward.

Drew Fenton: Today on behalf of CPA, we would like to thank Krist for your expert insights. I'm sure we have all discovered much more about cybersecurity in the not-for-profit sector. Thank you to all our listeners for tuning in to CPA Australia and Pitcher Partners podcast series on the not-for-profit sector. Please join us next time for a discussion on moving beyond cash, increasing returns without taking unnecessary risk. Another important topic for the sector.

Speaker 1: Thanks for listening to the CPA Australia podcast. To download the transcript and to find more information on today's episode, visit www.CPAAustralia.com.au/podcast/82