Interview Transcript

Interview conducted by Renee Gubbin and Jacqui Dilger, with Renee asking questions and Jacqui recording and editing the transcript.

Team HydroKnow gained the opportunity to interview an IT Professional of our choosing, and we were fortunate enough to have a close connection with substantial experience in the IT Field; Russell Close. Russell has been working in the IT field for nearly 30 years, meaning he has seen iteration after iteration of technology and the way that businesses mould around that. He is extremely well versed in anything IT, so the insight into not only IT as a field, but as a lifetime career, was phenomenal. Below you will find the interview transcript with time stamps that correspond to the recorded version of this interview. Questions have been highlighted for convenience.

[02:51] Renee: What exactly do you do?

> **[02:58] Russell**: *I'm Head of IT at Bennelong Funds Management. Bennelong is a Funds Management company. We have our core company called Bennelong, which has about 45 employees, and then we have a number of what we call 'boutiques' that we support. They're Fund Managers, so they buy and sell shares in the stock market. Bennelong provides sales, HR, accounting, IT, and all other services so that Fund Managers can pretty much just focus on managing the money and hopefully get really good returns for their investors.*

[03:43] Renee: Have you found that cryptocurrencies are becoming more relevant in your field?

> **[03:54] Russell**: *Look, not from our perspective. We have 6 boutiques, four of them invest in the Australian Stock Market, and two of them are international, but none of them are into Cryptocurrency. It's a fairly turbulent part of the investment landscape. They're mainly looking at trying to get value in small companies, large companies; for our internationals, they focus on infrastructure or real estate.*
>
> *So yeah, it's a good company to work for. I've been here for 7 years, so it's quite a stable place to work. We've grown a lot; when I started there were 38 people in total, and we've now got 85. We've also got a subsidiary over in the UK, and another small subsidiary that's just been set up in the US, so certainly growing. Which is exciting, good fun to be a part of it.*
>
> *My role; I look after everything to do with IT. That includes servers, software, cyber risks / cyber security, policy etc. So that's the whole- anything to do with IT and Information Security is under my remit. I've got two staff working for me. One is more of a database / developer, and the other fellow is more into support and learning more about the security side of things to support me in that area. We use a managed service provider for our desktop support, so they monitor and manage all of the servers and firewalls, and then they provide phone hook-up for desktop support. Myself and my two colleagues we sort of look after the business support and business applications and things like that. We do some internal development; in Funds Management there's a lot of systems out there that the fund managers will use to buy and sell the shares, but all these things have to talk to each other so we build the little interfaces between all of these systems, which is good.*

[06:31] Renee: So the industry you work in is sort of financial, but within IT?

> **[06:40] Russell**: *Yes. Finance; there's a lot of regulatory stuff that we have to meet. So, information security, cyber risk is the highest on the agenda at the moment. We have a number of companies that*

invest into our funds; superannuation funds, other companies that might want to put their super to our products, so we get a lot of due diligence requests and a lot of the focus for IT is all around managing cyber risk. There's things like business continuity; so if we have a disaster, can we recover? Can we get everything back up and running so that we don't lose time in the business and things like that? Obviously with Covid it's been a very practical and real example of business continuity, it was fascinating last year. We've done a lot of work in making sure our systems can support these sorts of things, but until you actually are in the situation, you never quite know how it's gonna go.

[07:51] Renee: And have to apply them, yeah. I guess that is the real test.

[07:54] Russell: *We went from the Thursday in March where everyone was in the office, to Friday where everyone was working from home. The transition was thankfully very smooth.*

[08:05] Renee: Oh that's good. I have heard some horror stories.

[08:08] Russell: *Yep, I've heard quite a lot of horror stories. You've got client information, so privacy is a huge thing; making sure we're protecting peoples personal information, and obviously with finance if you've opened up a bank account you realise you've got to provide ID, whether it's a drivers license or passport, date of birth, tax file numbers so obviously protecting that information is very critical. We've got to make sure we've got the appropriate controls in place to reduce that risk.*

[08:50] Renee: Do you think in that aspect cyber security has definitely had the most growth in the last 5 years / decade?

[08:57] Russell: *Definitely. We've always had to maintain security, but in terms of our clients questioning us, it's now top of the list from an IT perspective. With the superannuation industry, they've got a regulatory body called 'APRA' don't know if you've heard of them, but they've basically-*

[09:18] Renee: Yeah, in a medical term I've heard of them, but not for IT.

[09:22] Russell: *Yeah, so they monitor all of the superannuation companies and they've been rolling out a whole heap of regulatory requirements around cyber risk; and companies have to sort of make sure they're doing certain things in order to protect the client information, and that all flows down to us so it keeps us busy.*

[09:51] Renee: Now that you're working from home, do you specifically interact with anyone else from the workplace or is it mainly all other IT professionals?

[10:05] Russell: *No, no. We're only a small team of IT people, the three of us, so we use [Microsoft Teams] a lot, I can also access anybody's computer from my desk here, so we've got some tools to actually connect to their computer if we need to help with something. I can do exactly what I would normally do in the office, I just can't go and physically click on the mouse button; but having said that, If I'm connected to their laptop or PC, I can control the PC and do all those sorts of things that need to be done in order to help them keep working.*

For remote working we've got 2 mechanisms. Have you heard of a VPN (Virtual Private Network)? If it's a company owned laptop, then they can connect into the network using the VPN, but if they don't have a company laptop at home, they can connect into their workstation that's in the office, and that's using a remote desktop gateway. We run on the premise that if it's a work laptop, it's managed, we can monitor it, it's got all the appropriate anti-virus, anti-malware and controls on it, whereas if someone's accessing from their home computer / personal computer, we determine that unmanaged,

and so when they come in it sort of just opens up a session and that session can't actually communicate with the local PC, it sort of all happens within that session. It provides you with a level of security to make sure that if someone does happen to have something malicious on their home computer, it doesn't get into the work network.

[12:03] Renee: Do you have much to do with many of the clients or investors?

[12:08] Russell: *No, not the investors. So if I was to look at it like this, the boutiques are essentially my client. Whilst Bennelong owns part of their business, it's like me being a service provider to sort of provide that service to them. When we do the due diligence stuff which is sort of every one to two years with our bigger clients, I have to sit down and basically answer a whole heap of questions around how we manage our IT, how we manage cyber risk, how we manage business continuity and all those sorts of things. So that's sort of the only interaction I have with our end clients.*

[12:54] Renee: Do you spend most of your time interacting with everyone from the company then, in the IT department?

[13:03] Russell: *Being a smaller company, you sort of get to know everybody which is actually what I like. I've worked for big organisations, you [Renee] obviously have being in the army and all those sorts of things-*

[13:15] Renee: Yes, it's huge! Yep.

[13:18] Russell: *It's actually nice that I know everybody in the organisation, and from an IT support perspective that's actually quite advantageous because you know people's level of IT experience, and so you sort of can target how you instruct people to be able to do things or be able to fix things, you can sort of target it at their level of IT experience. It varies from people who actually have very very good IT skills, to those who have zero IT skills and struggle to even find the on/off button on a computer.*

[13:59] Renee: That would be my Mum. She's getting better.

[14:04] Russell: *You learn to be very patient.*

[14:07] Renee: Yes, and I think the Army has taught me that as well. The motto is hurry up and wait. But I mean I guess it has, I've kind of developed having patience with everything; not only just that aspect of waiting for something to happen, but yeah, I guess it's a good skill to have.

[14:31] Russell: *Even though some people don't have great IT skills, you don't wanna make them feel bad for that, because they've got skills in other areas that I don't have, so it's about that respect and just guiding people through the challenges they have. I'm in contact with at least a dozen people each day, generally to answer questions or help them with something and things like that.*

[15:05] Renee: So do you have a set time that you start work?

[15:10] Russell: *No, my hours are very flexible. I spent 2 and a half hours on Saturday doing some problem solving with a network issue, and 4 hours yesterday [Sunday] so the hours sort of tend to fluctuate. Sometimes I'm on at 9:30 at night helping someone with something, and you know other days I start work at 8:30 and finish at 4:30. It's very flexible. It helps when you've worked with someone, with a company for a long time. A number of people I work with here at Bennelong I've actually worked with previously, so people sort of know how you work and that you're going to get*

the job done. So you've sort of got that understanding that it'll get done when it needs to get done, and we've got that flexibility if you want to take 2 hours off in the middle of the day and go on a bike ride then that's quite flexible as well.

[16:11] Renee: Yeah, it sounds great. It's almost like a dream career; you're like 'ooh', there's so much flexibility involved. It works with everyone now, since COVID and being able to work from home. It provides flexibility with family as well.

[16:28] Russell: *Yep. One of my staff members has two young children, and obviously they've had to do home schooling and stuff like that. Our CEO is fantastic, and he's very much 'look, we understand it's a difficult time, if you need to take 3 hours out of the middle of the day because you've got a little one to look after, that's fine'. For a job to be done, as long as people get it done, someone might take 2 hours or someone might take 4 hours, at the end of the day It's about making sure that we can keep everything going and people get what they need to get.*

[17:07] Renee: Is there anything that's probably more challenging in your work?

[17:13] Russell: *Look, cyber is the real challenge. There's so many ways a company can be attacked from a cyber perspective, I think that you can never sit back and say 'yep we're okay' because it's always changing, and it's always trying to keep up with that change to make sure we're maintaining the security of that environment and reducing the risks that continue to come against us, so that to me is the biggest challenge. It's good, and it doesn't keep me awake too many times during the week, but sometimes it does. You're dealing with, especially now with COVID where you've got 85 people all working remotely, it obviously increases the risk. Sort of being able to manage that and maintain that. We've got tools in place that help us manage those sorts of things, we've got part of the Microsoft Suite called Intune, which allows you to actually monitor mobile devices (that being laptops and mobile phones and things like that), and at least ensure that they're remaining secure. Not so much that they're watching what people are doing, it's just that if something is not in place that should be in place, it actually lets us know, so that certainly helps a lot, but it's just constantly evolving.*

[18:52] Renee: From what you know, is there anything that these attacks are wanting? Is it personal data?

[19:03] Russell: *Most of these attacks seem to be opportunistic. You look at other companies and what's happened where they try and get in and it is stealing people's personal information so that they can potentially use that; obviously if you're a bank they're after credit card information, or if they're a small business that does online transactions. That's always one of the biggest risks when we purchase things over the internet, you don't know how well the person you're buying it off is actually managing and maintaining their systems, so yeah, it's always good to be careful with those sorts of things. I think in our situation, they'd probably try and get peoples email credentials and things like that, and then try and syphon off information or to then perhaps try and get someone to make a payment or things like that, that's probably our biggest one. We've got things in place to monitor for those sorts of things which is good; multifactor authentication on everything that we can because that reduces 95% of your risk, if you've got to get that alert on your phone or a 6-digit code, it's hard for someone to actually get into your email if they don't have the second factor. I encourage all of my staff, if you can turn multi-factor on, turn it on. It does reduce a lot of the risk.*

[20:47] Renee: Are there any memories from working in IT that could be captured? A positive or negative experience?

[21:03] Russell: *That's an interesting question. Look, I love working in IT, I'm up to nearly 30 years now, so I've done a lot of development work and quite enjoyed doing development work. It's one of*

the things that I love about this job; yes I'm managing IT and looking after all of it at that top level, but I also get to write code, write programs, do all of the lower detail type stuff, which I get a lot of reward out of doing. I think if you can deliver something that's going to help people do their job better, that's really rewarding. Job difficulties, hmm. There's been a couple of contracts that I did earlier on in my career that're just terrible. I think that if you can find a good company, you potentially just stay there your whole career. Culture, how people relate to each other, those sorts of things are one of my important things, rather than earning lots of money. In IT, I've had experiences where you're working with some fairly interesting characters from an IT perspective and yeah, that's probably a difficulty I've found; but in terms of just actually doing the IT side of things it's been great.

[22:42] Renee: Yeah, meet a lot of great people along the way as well.

[22:46] Russell: *And being able to actually work with the business, the people who are not in IT, you learn a lot about the business and sort of get a better understanding of what you're helping them with. I think that is also very rewarding, and you can actually understand why you're doing something.*

[23:10] Renee: Can you share an example of the work that you do, or that best captures the essence of the IT Industry?

[23:18] Russell: *There's just so many areas in IT now. If you focused on Cyber Security, that in itself is a career path in itself. If you decide to go down the software development path, again, it's challenging. Once you're in that area it's hard to get out of it. …How would I describe IT? I guess when you step back, it's about making sure that people can do what they need to do. As we mentioned before, there are people who have a good understanding of IT, and there's a lot of people who don't have a good understanding of IT, and I think people can be quite scared that they're going to something wrong and that it'll all go really bad, so I think the IT Industry is about enabling people to do what they need to do without having to worry about the technology, because it can be a scary thing if something goes wrong and you don't know how to fix it. It's about enabling people to do their job.*

[24:38] Renee: Yep. I think I was explaining IT my now 89 year old grandmother, and I said 'Nana, IT is kind of like your asthma. It's like an umbrella term now that we use. I didn't even get started into what Cloud Computing was, I didn't want to scare her off. She's got an iPhone and she just knows that sometimes her messages are blue, and sometimes they're green.

[25:16] Russell: *The fact that she knows that they're blue and green and that might mean something slightly different; that's actually pretty impressive.*

[25:24] Renee: It is! She knows that she can send a message from home for free using her wifi; yeah, she's very cluey though. She used to work on the switchboard at the GPO in Sydney.

[25:41] Russell: *Yeah, I mean it's pretty scary for people who are in their 70s and 80s to try and get their head around these things, and how they actually work. I don't think there's always a lot of thought given into people who haven't grown up with technology and how hard it is to get the understanding you need to be able to use it.*

[26:08] Renee: Because it is, it's a lot of not just professional development, but a lot of personal development that you have to continue to do.

[26:21] Russell: *Yeah, Yep.*

[26:24] Renee: What do you think the IT Industry has in store for it within the next few years?

[26:31] Russell: *It's an interesting one. I look at say Australia in the last 10 – 15 years, there's been a shift to outsourcing, where everything's outsourced to service providers and things like that. I think with what's happened with COVID, there could actually be more of a move to bring people back into the business. Companies need to have people in the business who actually understand how it all works, and can provide that sort of buffer between the business people, the end users, and the actual technology. Even though you've got a lot more new technologies coming out that do make some things easier, in some ways they do make it more complicated. You've sort of got to configure these things and actually make them work; providing they work that's great, but it's when they don't work- that's where it gets really complicated. Having someone at the other end of the phone who doesn't really know anything about you as a person, trying to explain to you how to fix something, I think that's a good challenge. Especially for small to medium size businesses, they're going to want someone on the ground who can actually do those sorts of things. Everyone talks about the cloud and all those sorts of things; obviously there will be more and more of that, but it depends on where you end up working. The risks are going to continue from a cyber risk perspective, and that's going to be the area that has to continue to grow. The attackers are getting more and more sophisticated, and so I think there could be some real challenges in the coming 5 – 10 years in terms of attacks and what they're able to do. I think the business is going to have to evolve to continue to meet that challenge. There'll be more Internet of Things, more smart devices and all this sort of stuff. I don't think that's ever going to end. But the short term will be more of the same. Again, with COVID, it just depends on what happens over the next 12 – 18 months; as things start to open up and allow people to sort of start to live life normally, I guess we'll get a better idea of which way things are going to go.*

[29:24] Renee: It's almost been like that already, everything's had to be fast-forwarded so quickly.

[29:32] Russell: *Cyber Risk is the big one. It's certainly been growing the last 5 years, and I think it's going to continue to grow. The thing about cloud computing and all those sorts of things, the more you host things on the public cloud, the greater the risk. If you've got your systems inside an office with proper firewalls and things like that, there's far less attack methods whereas once everything's sitting up in the cloud, you're then losing that control over the management and relying on the third parties to actually remain safe and secure.*

[30:20] Renee: It's almost kind of scary in a way, that it's just going to in a way get worse as we move forward.

[30:31] Russell: Yeah. I think back on when I started working and there was no such thing as the internet, you had servers and computers inside the organisation, and the whole thing about a virus just did not exist. The more public we get, the more connected we get; the more risk that we're creating. Cyber is probably a good growth area to move into.

[31:06] Renee: I think it's interesting from all aspects. I look at things from my personal perspective and having a lot of friends who put their children on social media and what they do with photos and images and stuff, all that data scares me. I think we're not there yet, we don't know how much of a footprint we're leaving for our children or if that'll be detrimental to their future. We have no idea.

[31:36] Russell: Yeah. I think that is challenging. The moment that you post it, you no longer own it, you know? We know that these big organisations data mine and they've got some very sophisticated processes that can actually look at all this data and start to put it together and create profiles on people. That's why you do searches on Google and next time you go in, 'ah!', it pops up with a different organisation selling something that you were looking at yesterday.

[32:12] Renee: Yes! And selling all of our data. I don't even know how many spam calls I get saying 'oh, change your electricity provider!' and I'm just like, oh my god. I continuously block calls or day.

[32:30] Russell: Yep, I don't answer my phone if I don't recognise the number. Which is a shame really, it just becomes a real interruption into your day-to-day living. I think that's going to continue. Those who are trying to benefit from these things are getting more and more sophisticated and smarter about how they do it. It's gonna be a fun ride.

[33:03] Renee: Maybe Jacqui and I have made a really good decision to move in now, and Will as well.

[33:09] Russell: Yeah, I think so. I think that it dropped off for a while, people weren't going into IT, but I think there's going to be some great opportunities to really establish yourself in a good career.

[33:27] Renee: Well thank you so much for chatting with Jacqui and I; I just can't believe how much information you've provided us with, it's great. I will stick with Cyber Security then!

[33:40] Russell: Yeah, well see how you go with your course; you might go into a different area and go 'oh wow, I really like this too' but if you can sort of give yourself options, I think that's always a good thing. I did a degree a few years ago that was hardware and software, and interestingly I focused more on hardware when I was doing my degree but ended up on the software side of things, and it just goes from there. It's been great. There's not really been any times where I haven't really enjoyed what I'm doing. I like solving problems, and I like helping people.