accenture

Hear+Beyond

Accelerating Australian Business

To access other episodes in the series, click here.

SEASON 1, EPISODE 2 TRANSCRIPT

Andy Penn on Australia's new cybersecurity landscape

HOST: Rae Johnston, Multi Award-Winning Australian Journalist
GUEST: Andy Penn, CEO, Telstra

Rae: Hi, and welcome to Hear+Beyond, a podcast brought to you by Accenture. This series is a must-listen if, like me, you're curious about the future of Australian business beyond a pandemic. I'm Rae Johnston, and I'm here to ask the hard questions on the topics that really matter. I'll be joined by prominent business leaders who share their thinking around how Australia can accelerate business from here and beyond.

Voice Over: Hear+Beyond. Accelerating Australian business.

Rae: I'm joined today by Andy Penn, CEO of Telstra, who's here to talk about the future of Australia's digital economy, and the importance of its security to drive success. Andy has been at Telstra for almost nine years now, but his 40 year long career has also seen him work in financial services and in shipping. He's heavily involved in cybersecurity. He was chair of the Industry Advisory Panel, which assisted the development of Australia's 2020 Cybersecurity Strategy. Andy has also recently been appointed chair of the Industry Advisory Committee, which will guide the implementation of this 2020 strategy. The security landscape has been evolving fast recently, but now it's morphing at breakneck speed. I want to know what challenges lie ahead for Australia and how can we as a nation overcome these challenges to realise a more secure future? Let's find out. Hi Andy, and welcome to Hear+Beyond.

Andy: Hi Rae, it's great to be here.

Rae: Now, you're in Melbourne at the moment on its way out of a COVID induced locked down. How have you been coping? How are you feeling now?

Andy: I'm feeling pretty good. It's been a tough six or seven months, I have to say because Victoria, unfortunately, in Australia had the highest incidence of positive cases and as a consequence, the restrictions that were put in place for pretty onerous. I feel as though I've been under house arrest for the last three months, but the good news is we can see the light at the end of the tunnel and things are starting to open up, which is fantastic.

Rae: Did you pick up any hobbies or fun working from home habits that you'd like to share?

Andy: Well, I'm a bit fitter, that's a good thing. So, I've been able to get my exercise in. I think I'm benefiting from the lack of commute time and I normally paint in my spare time. So that's actually one of the things I've missed because my art studio is not in the same location as my home, and so I can't actually get to my art studio at the moment. That restriction is lifting in a couple of weeks, so I'm looking forward to doing that.

Rae: Sounds amazing. Now we are here to talk a little about cybersecurity and I'd like to know from you what the impacts of lockdown and the pandemic have been from a cybersecurity standpoint, what's changed?

Andy: Thanks Rae. Well, it's been a very important and profound time from a cybersecurity perspective over the last six or seven months, and really I'd say three things. Firstly, as we have all moved to work and study from home and we've done more things online out of necessity because of the restrictions, it follows obviously the level of cyber risk has increased just because we're doing more stuff online. More e-commerce, more studying, more learning, more business online. I think the second thing is that as we have all moved to work and study from home as well in many respects, we've moved outside of our normal security environment. In some respects that might mean outside of the normal firewalls.

In our respect at Telstra, we're still operating and many big companies are still operating within their own private networks with VPNs, but that's not the case for everybody and in any event we have certain protocols in certain parts of our businesses and buildings that enhance our level of cyber protection. And then the third thing is that malicious cyber actors have taken advantage of this, and we have definitely seen a very significant increase in the level of malicious activity in the cyber space. I mean, for example, if you look at Accenture's Cyber Threatscape research released not long ago where there's a 60% increase in the average ransom payments in the first quarter of 2020, we've seen a very significant increase in the level of malicious activity.

We've blocked about 50 malicious COVID-19 themed domains, so people, malicious actors purporting to be sending you something which is COVID related and looks important, but which is not actually. It's got malicious content in it and it's not just criminals. We've also seen a very significant increase in state-based cyber activity as well. So, it's been a pretty significant period for cyber.

Rae: Why is there that increase in that scam-like activity?

Andy: I just think that malicious actors have seen that people are more online. They are outside of their normal security protocols in some respects, and they're exploiting that opportunity. And, I think, it plays into the broader dynamic about cyber activity and cybercrime is that, unfortunately, the rewards are potentially very significant, whether that be financially for criminals or strategically for nation states, and the consequences aren't very material. So, you can get away with it. I like to say that in the olden days, if you wanted to rob a bank, you literally had to physically go to the bank and hold it up and get the money out of the safe, and of course, if you got caught, well then you got put in jail.

Whereas now you can rob a bank from the other side of the world. And even if you get caught, the consequences aren't significant, because the likelihood is, you're actually located in a jurisdiction that's not going to do anything about it anyway. And so that's one of the unfortunate things about cyber, it's the consequences are very small, and the rewards are very high and there's a lot of malicious actors out there that are taking advantage of that.

Rae: So, considering the increase in reliance of being online for your healthcare, and working from home, and education, and entertainment, and the internet essentially being the cornerstone of our economy. How does thinking around security need to change in a post-pandemic world?

Andy: Well, it's interesting actually, because the Australian government set up a review of its cybersecurity strategy, to lead to a new cybersecurity strategy for 2020 and beyond, and commenced that process late last year and asked me to chair their advisory panel for the development of that strategy. Which is what I've been doing and I'm now going to chair the panel that oversees the implementation of the initiatives, but it was interesting because we were doing that before COVID struck and then COVID struck, and so it added an extra dimension to it. The simple point is that many countries are looking to use the digital economy as a way for a fast-economic recovery from COVID. But it means by definition, if we're going to do more things online, we need to build the cyber defences to be commensurate with that.

That's what the Australian cybersecurity strategy is fundamentally aimed at doing. The way in which we've looked at it, we've looked at it through three sets of stakeholders. So there's government, and then there's businesses, and then there's consumers and citizens. Fundamentally, what the strategy says is the government needs to focus on firstly being an exemplar in relation to cyber defences in its own operations. So, Department of Health or Department of Human Services, or Department of Defence, whatever the government is doing, it needs to be an exemplar in protecting its own activities, one. But then two, the government also has a role to play in what we call critical infrastructure and systems of national significance.

So there are things like telecommunications, or banking, or power, or food supply. If those systems get interrupted, even when they're managed by the private sector, if they get interrupted nonetheless, it's a national security risk and the government has to have the ability to step in and play a role in defending those assets. That's the role of government. What we looked at is in relation to the role of business is that we need to lift the level of responsibility of businesses that are providing digital products and services to ensure that those digital products and services are safe and secure. So, if it's an internet connected fridge or an internet connected baby monitor or whatever it may be, they need to be cyber safe and cyber secure, so they can't be exploited.

Finally, for consumers or the citizens, there is always going to be an element of caveat emptor, they'll always be a responsibility that citizens and individuals need to take. Therefore, we need to lift the level of awareness of what constitutes being safe when we're working on the internet, it's the whole big awareness program that flows from it. So it was actually very timely for us that we were working on a 2020 cybersecurity strategy at the time that COVID hit, because COVID hasn't really changed anything. It's just reinforced the importance and the criticality of these initiatives.

Rae: You've talked about how important cyber security is obviously, but you've also talked about the huge amount of challenges that Australian businesses are facing now and also into the future. But when you've got, for example, 43% of companies saying that cybersecurity costs have increased for them in the last two years, and 70% saying that they find those costs unsustainable. What does that mean for the priority cybersecurity investment should take in their budgets?

Andy: The flip side of that is that the digital economy and digitisation actually also offers opportunity. So opportunities to reach new markets, opportunities to reach new customers, opportunities to redesign processes and run them far more efficiently, and so I think cyber security and digitisation go hand in glove and they go together. What COVID has shown is that there are very material opportunities for businesses to transform digitally for their benefit, because what we're seeing is a greater adoption of doing business digitally. In fact, if I look back and reflect on the last six months, we've seen more digital adoption from customers and from businesses and from stakeholders in the last six months than we have in the previous five years. The interesting thing about that to me, is it says that technology wasn't the constraint previously, because if technology was the constraint, we wouldn't have been able to adopt it as quickly because it would have taken longer to build.

Andy: So, actually what it has been is, it's been more our willingness or ability or our propensity to do things digitally that has changed. I don't think that's going to go back. So, the point is that there are opportunities for businesses to accelerate their digital programs. Unfortunately, though, what goes hand in glove with that is it's also important to build your cyber defences and cyber capabilities commensurate with that opportunity. There are, again for us in Australia and the work that we're doing with the Australian government on the 2020 cybersecurity strategy, there's a lot of initiatives actually that are aimed at particularly small business to help small business in this journey of protecting themselves from a cyber perspective.

Rae: Now, obviously we're going to need a pretty strong workforce, with a lot of skilled cyber security professionals for our digital economy and our security both now and into the future. But is talent going to keep up with demand or do you foresee a skills deficit?

Andy: Certainly, in Australia, there is a challenge, not just in cyber skills, but in digital skills more generally. According to the OECD report, one, the proportion of new students entering STEAM based degrees in Australia is about 21% compared to 27% in other OECD countries. And we see that as Telstra is probably the biggest technology company in the country, the number of IT grads and software development engineers and robotics engineers, and cybersecurity experts that we need is definitely a challenge. And we are working in partnership with a number of the universities to try and help develop curriculums and develop initiatives to improve that pipeline. The one thing I would say though, is that yes, we need more cybersecurity experts, but actually probably a bigger issue is to build cybersecurity skills into existing technology programs.

In other words, to make sure that there's the appropriate level of cybersecurity education and learning in the programs for robotics engineers, for software engineers, for data scientists. In fact, that's where we actually see a bigger gap and that's actually a faster opportunity. We have software engineers that we recruit that are not as cyber literate as they should be given that they're software engineers. That's actually where we can get a faster difference or have a faster impact as well as just the deep, deep cyber experts.

Rae: That makes a lot of sense, and I think it would also make sense for ongoing training to be something, because whatever you're learning in your formal education is often obsolete by the time you graduate.

Andy: I think that's absolutely right and there's a lot of talk these days about micro-credentials and as you say much more bite-sized learnings, and it's not just necessarily for software engineers and other engineers, it's for all of us. The more things that we do online, the more it beholds us all to lift our level of awareness of what constitutes doing things safely online. I often analogise things in the digital world to things in the physical world, because the challenge in the digital world and cyber, it all sounds very mysterious and hard to conceptualise.

Rae: It's witchcraft.

Andy: Well it is, because it's intangible, but actually most things that we do in the digital world are just a reflection of what we used to do in the physical world. And if we did them in the physical world, it's a lot more obvious because you can sense by virtue of your feelings about what you see and what you hear and what you touch and smell. You can sense things and so it makes sense. So, in other words you would not go down a dark alley at two o'clock in the morning in a city somewhere in the world that you've never been to before. You just wouldn't do it.

Andy: So, the question is, are you doing that online? How do you know whether you're doing that online? And so, it's those sort of analogies that might be helpful in people understanding and being a little bit more thoughtful about how they're interacting digitally, and what they're doing, and when they're clicking a link. Just really asking themselves the question, do I really want to go down this alleyway? What is there that's around this that is telling me that's the safe place to be? But I do see that learning will develop over time.

Rae: So, what should Australian companies looking to make the smartest investment possible in cybersecurity... What should they be thinking about?

Andy: A lot of companies tend to think of cybersecurity through the lens of technology, or rather the technology is the solution because it's digital, it must mean that technology is the solution. Actually, overwhelmingly, cyber vulnerabilities arise as a consequence of poor process and individual behaviours. In other words, it's people clicking a link that they shouldn't or picking up a USB that they don't know where it came from and putting it in their computer or processes which don't afford appropriate protection and build in appropriate protection. My point being is that companies need to look at all of those things. They need to... Yes they need to look at the technology and as innovation progresses, the cyber actors get more sophisticated, you need more sophisticated technology to protect against that, but also reviewing processes and educating employees and customers to be much more alert to where cyber risks maybe occur.

So good disciplines around passwords is another good example. Candidly, I think the day of passwords is fast coming to an end, it is not a safe way to protect yourself online and we're going to need to move to biometrics increasingly. But in the meantime, 98%, 99% of passwords around the world are very, very easy to guess and to hack quite frankly, just by you go on somebody's Facebook site, you can probably work out their password pretty quickly.

Rae: It's probably “password”, statistically.

Andy: It's probably, or it's their favourite dog's name and coupled with their date of birth or their birthday or their age, it's not hard to work out.

Rae: Terrifying. Get a password manager people, come on. So, the challenges that lie ahead. They're pretty significant. Are you optimistic about the prospects of keeping Australia secure online?

Andy: Absolutely, because I'm optimistic about what a digital economy can really do for a country particularly, and that's only been brought into sharp focus as a consequence of COVID. Therefore, if you've got an advanced digital economy, which is the cyber safe economy, then relatively speaking compared against the rest of the world, you're in a very strong position. Similarly, if you're a company, if you're very digitally enabled and you've got good cyber security, then you're in an excellent position. And so it's not a case of protecting against or guaranteeing that you're never going to have an incident. The reality is you are. The question is, can you build enough protection in to give people confidence that they want to do business with you rather than your competitor, because this is a relative game. It's not an absolute game.

I'm proud to have worked on the Australia's cybersecurity strategy and now to be heavily involved in overseeing the implementation of it. Because I think if we... It's a $1.7 billion investment in enhancing our cyber defences nationally. If we can do that well, coupled with meeting the aspirations of the government to develop a, or to develop Australia into a leading digital economy over the next decade, then I think that puts us in an incredibly strong position competitively.

Rae: Fantastic to hear. Thank you so much for your time Andy.

Andy: Thank you very much Rae. It's been great to speak, and thank you for the opportunity.

Rae: You can find out more about the stats and figures. Andy and I discussed in the show notes at accenture.com/hear+beyond. There's so much more coming up in the series from responsible business to supply chain resilience. You can catch the next episode of Hear+Beyond where I'll be joined by Anna Bligh.

Voice Over: Hear+Beyond. Accelerating Australian business.

Rae: You can listen to Accenture's Hear+Beyond podcast series from Spotify, Apple, Google, or wherever you get your podcasts. Thanks for listening and don't forget to subscribe.

[End of recording.]

To access other episodes in the Hear+Beyond series, click here.