IPAA ACT
INSTITUTE OF
PUBLIC ADMINISTRATION
AUSTRALIA

02 6154 9800
PO Box 4349 Kingston ACT 2604
admin@act.ipaa.org.au
www.act.ipaa.org.au

ABN 24 656 727 375

TRANSCRIPT OF PODCAST

WORK WITH PURPOSE
EPISODE 32

HAMISH HANSFORD
Cyber, Digital and Technology Policy Division
Department of Home Affairs

Hosted by DAVID PEMBROKE, Founder and Chief Executive Officer, contentgroup

1 February 2021

Enquiries should be directed to Caroline Walsh on 0413 139 427 or at caroline.walsh@act.ipaa.org.au

Delivered in a partnership between IPAA ACT and contentgroup

contentgroup

DAVID PEMBROKE: Hello, ladies and gentlemen, and welcome to Work with Purpose. A podcast about the Australian Public Service. My name's David Pembroke. Thanks for joining me. I begin today's podcast by acknowledging the traditional custodians of the land on which we meet today, the Ngunnawal people, and pay my respects to their Elders past, present, and emerging, and acknowledge the ongoing contribution they make to the life of our city and this region.

Well we're back, fit and ready to go for 2021 and another year of great conversations with the leaders of the Australian Public Service. Context is always important, and it's fair to say that we begin this new year with more than a little doubt about what lies ahead of us. But whichever way it falls, the influence and importance of the Australian Public Service to the Australian people will continue to grow. Government will be more a part of the lives of Australian citizens than perhaps at any other times since the war.

And it will be the APS who connects citizens and their elected leaders through the delivery of services, policy, program, and regulation. Now, aside from dealing with the ongoing challenge of the COVID-19 pandemic, cyber security is right at the top of the list of things we are all worried about. Who can forget last year's announcement by the Prime Minister in June, that Australia was being targeted by a sophisticated state-based actor, and Defence Minister Linda Reynolds' description of the persistent cyber attacks on Australia as being in a grey zone that blurs the line between peace and war.

Now, while COVID-19 has presented many public health challenges, it has also forced more people online. More people are, and will, continue to work from home, more people will be spending more time online and our once secured computing services are now being moved from a server to the cloud. The Australian Cyber Security Centre estimates that there are an average of 164 cyber crimes each day, while some suspect that that number is well under-reported.

Now in the face of all of this overwhelming and persistent threat, the Australian government has invested heavily, $1.7 billion in the national Cyber Security Strategy, with investment in workforce, skills, partnerships, technology, industry engagement, research, innovation, and of course, with defence. Now while one of the key mantras of cyber security is that it is everyone's job, someone with a little more responsibility than most is Hamish Hansford, who is the First Assistant Secretary of Cyber, Digital and Technology Policy division at the Department of Home Affairs.

In this role, Hamish leads Australia's cyber security and cyber crime policy, the online harms policy, which includes countering terrorism and child exploitation, encryption policy, as well as technology security policy. He has had a long career in cyber and in security, and he joins me in Studio-19, Hamish, welcome to Work with Purpose.

HAMISH HANSFORD: Well, thank you very much. It's good to be here.

DAVID PEMBROKE: Happy New Year.

HAMISH HANSFORD: Likewise. 2021 is going to be great.

DAVID PEMBROKE: Did you get a break?

HAMISH HANSFORD: I did. Got to get down the coast for a little bit and then back into it now.

DAVID PEMBROKE: How do you decompress? Because this job that you have, when you line up all of those things, it seems to me that it would be a job that your phone is never too far from your hand and you are always on.

HAMISH HANSFORD: That's right. 2020 was a pretty big year for cyber security and I delivered a range of things with colleagues across the Commonwealth, and it was pretty busy but it's always good to take a break at the end of the year. And as you judged by the news cycle, it got pretty quiet over Christmas. So that was a good thing compared to last year.

DAVID PEMBROKE: Yeah. But how do you manage yourself during those really hyperactive periods where it is so busy? Because I think we do have to think more about mental health and looking after people, and really being able to maintain what is such great pressure when you consider the sorts of pressures that you're under.

HAMISH HANSFORD: Exactly. I think that it's really good to start the day with exercise, it really changes your mental focus and agility throughout the day. During a crisis it's really good to focus on and consistently revisit your priorities to make sure that you're focusing on the right things and pushing things forward. But you're right, it is a bit of a challenge.

DAVID PEMBROKE: What about your teams? How do you manage your teams when obviously there's pressure on them to deliver as well?

HAMISH HANSFORD: Exactly. Really looking at mental health, encouraging, motivating, making sure that people are really okay in the workplace, and where you do see fatigue, you have to make a conscious choice to rest people despite the priorities that might exist, and really looking out for each other and working as a team, I think is the best way to go. And COVID-19 demonstrated that in abundance. We tried to do new things, working on things from shutting down the Australian border for the first time, right through to trying to prevent PPE from leaving the country. So we did really new things and touching base more often, particularly those working from home. One of the ways we tried to touch base was have a really quick meeting every day, via video conference or teleconference, to make sure that everyone was working on the highest priority issues. We were connected and making sure that everyone was okay.

DAVID PEMBROKE: So how did you go with working from home? Did you work from home?

HAMISH HANSFORD: I did. I did bits of working from home and it was challenging trying to manage a two year old and a 10 year old, both homeschooling, and it was great that in Canberra daycares didn't close down. So it was a bit more of a balance, but I think you change your working hours somewhat and you change your working style. You really got used to having kids screaming in the background at the end of a video conference, and it was a different way of working.

DAVID PEMBROKE: How did it change you? What do you take from 2020 into 2021, that's going to make you a better leader.

HAMISH HANSFORD: I think the agility to change to different priorities. I think that's a really defining feature of 2020, dealing with COVID-19, and then in many cases, doing your day job on top. I think that really, you've got to be really agile and really consistently looking at the environment and situational awareness, watching national cabinet press conferences after the prime minister stood up after the national cabinet, making sure you're in touch with people. I think consistently, communications as a pretty big theme of 2020. And you mentioned at the beginning, we all went online and that's changed the way that we've worked with international partners, with industry and in how we work every day with colleagues across the Commonwealth.

DAVID PEMBROKE: Now, in the introduction, I described what you do in terms of your responsibilities, but can you explain to us, perhaps in plain English, just exactly what your responsibility is in the role that you have?

HAMISH HANSFORD: So I've got cyber security policy for Australia, looking at how do you build a much more cyber secure economy? And increasingly we're working on the flip side of departments like the Department of Industry, or the Treasury, who are building the economic future of Australia and a more digital Australia, including Prime Minister and Cabinet. And we're looking at the flip side of, how do you make a secure digital economy into the future, and how do you try and make Australia, with so many people more online and so many businesses online and engaging with the rest of the world, it's great to have such prosperity online, but dealing with the flip side on cyber security. I also look at the online content, so the criminal acts that are occurring online, how do you look to prevent that? The Prime Minister has consistently said, "The rules in the physical world should apply in the online world."

And so when you think that through it, it's really about an international coalition of, "How do you build online laws and rules?" And that is a global challenge, and one that's a particular relevance in our space with America, and how do you work with the United States government to change the rules online? And then finally, technology security. How do you create great domestic technology, lots of software developers in Australia, lots of critical technology that Australia is leading edge in terms of global competition. How do you build security into our technology, either from a research perspective or from commercialisation?

DAVID PEMBROKE: So it sounds like we are perpetually under siege. Now, those of us who are not in the business, so to speak, probably don't see, or don't see as much as we are, but is it as bad as those numbers suggested in the introduction?

HAMISH HANSFORD: That's right. One cyber crime report every 10 minutes to the ACSC, and I really think that's a good insight into the volume of crime that's occurring online. And cyber crime, you only need to look at your emails and the malicious links that you get from cyber criminals to realise that, particularly during COVID-19, when there's so many people online, it's a really easy way for criminals to earn money and target Australians.

DAVID PEMBROKE: But it just seems to me to be such a big problem. So how well on top of it, do you feel that Australia is? How well prepared or how well are we doing in the war, in the cyber security war?

HAMISH HANSFORD: Well, I think you mentioned at the beginning, the $1.67 billion investment by the government, and that really... When you look at cyber security in Australia, one of the big policy issues that the government was considering last year was around critical infrastructure. So how do you build cyber security resilience into really critical things that make our economy function? So the government's introduced legislation into the parliament to really focus on uplift of critical infrastructure security that should have, assuming that parliament passes legislation, a flow-down effect to then on to all Australians to make sure that they have confidence in critical infrastructure.

Lots of investment in industry support, either awareness raising or collaboration with industry, to try and uplift cyber security. But you also mentioned, and you're right that the missing ingredient is often you, the individual Australian. And trying to make sure that everyone is much more cyber literate, understanding what data you put online, what compromise that might lead you to then having, in a future life, being very cautious about not trusting either content or links or cyber security known methodologies that people exploit online. So being much more cautious, I think, in engaging in an online world.

DAVID PEMBROKE: Do you think we are becoming more cautious? Is behaviour changing? Are you seeing that behaviour change?

HAMISH HANSFORD: I think that naturally when you see the volume of, particularly cyber crime in your inbox, I think people are becoming pretty suspicious and criminals are becoming increasingly sophisticated and pretty quickly use the COVID-19 experience to change a lot of their scams to have a COVID-19 theme, and timed it really precisely with some of the announcements by governments around the world, including in Australia. So they're pretty entrepreneurial, and I think it's really difficult sometimes to work out the difference between a scam, or something that has criminal intent, and a legitimate advertisement from a company or a legitimate warning from a from a banker or telecommunications company.

DAVID PEMBROKE: I'm interested to know, because you did reference that $1.6 billion package in the national Cyber Security Strategy and all of those components that went into quite a complex package that was all put together. From a public servant's point of view, operating as you were remotely with all of the challenges of consultation and both with industry and overseas and everywhere else, just how hard was it to maintain that work pattern and program, to be able to ultimately deliver the strategy and the program?

HAMISH HANSFORD: I think any whole of government effort is often quite difficult, but actually, in kind of a perverse way, having to move online meant you can do more meetings. You don't have to factor in travel time, you can get out and talk to industry representatives. And we had an industry advisory panel chaired by Andy Penn, who I know has come to IPAA before and give a talk, and connecting with him virtually was much easier than trying to go to a different state. So perversely, I think we actually spoke to a lot more people across government and a lot more industry representatives, particularly with the critical infrastructure reforms, that we could talk to 3,000 people about the new reforms that the government asked us to deliver, and really lots of town halls that we hadn't done before online. And you see lots more engagement. People are often more willing to write questions than speak up in a large group. So I think in a kind of a perverse way, we had much more engagement than we perhaps would have otherwise.

DAVID PEMBROKE: And into the future, you'll obviously retain a lot of this work practice that has been developed through 2020.

HAMISH HANSFORD: I think that's right. You do miss something having face-to-face communications, but you can cover a lot more ground and the amount of podcasts and webinars and town hall meetings we've done online mean we get a much diverse, a much more diverse view, and we can reach much more people at a fraction of the cost than travelling across Australia and indeed internationally.

DAVID PEMBROKE: So it's fair to say, you've got a better outcome.

HAMISH HANSFORD: I think that's right. I think we spoke to more people, so we had a richer evidence base for some of the reforms that we developed last year.

DAVID PEMBROKE: Excellent. Now I know you're a keen listener of the Work with Purpose podcast, but one of the features of the podcast is that we hear from members of the IPAA's Future Leaders committee. And I've got a couple of questions here for you, Hamish. And the first of those comes from Jack Milne, from the Attorney-General's Department. And Jack asks, "You have worked in a range of roles and held leadership roles throughout your APS career, how can we embrace mobility throughout our career, and how can we create a workplace culture that supports it?"

HAMISH HANSFORD: So I got some pretty early advice from some senior mentors and they indicated you've got two paths in the Australian Public Service. You can either stay in one department or agency or one field and specialise, or take the opportunity to move around the public service and really get to understand how government works from multiple perspectives.

So I started as an APS two in the National Museum of Australia almost 20 years ago, and since then I've been in nine different departments or agencies across the Commonwealth, and always learnt new things and met lots of people across the Commonwealth and lots of different agencies. And I think that's helped me build a strong understanding of government and a strong understanding of lots of people across government and a good network.

It's really interesting, Bill Gates is recommended one of the books, it's called *Range*, it's about how the generalists actually advance economies and governments and society. And I think I've taken a lot of inspiration from that book around, "How can you be a generalist with specific knowledge to be able to succeed?" And I think that's one pathway, but equally, other people have different specialisations and they're equally as valid.

DAVID PEMBROKE: When did you discover security? Because that seems to have been a theme. Were you a security guard at the National Museum?

HAMISH HANSFORD: Right. I was a tour guide there and it was a fantastic job and one that I'd recommend for anyone, but then I moved into transport security and then did a national security role in Prime Minister and Cabinet, and then picked up the same theme in Attorney-Generals' from a criminal justice perspective, and then worked on the National Broadband Network and went up to Parliament House for a bit and then came down and I've had either community protection, criminal justice or national security roles in Home Affairs, Immigration, and the Australian Criminal Intelligence Commission.

DAVID PEMBROKE: But I suppose, maybe Jack's question is, "Did you follow your nose, or were you seeking guidance all the way through or was it, 'Gee, that looks interesting. I think I might just go over and spend a bit of time over there.'" So, accident more than design?

HAMISH HANSFORD: Yeah. I think once you get to know many more people, you kind of talk to people about different roles, and I think I moved to interesting roles with people that inspired me or I liked to working with. So I think I've moved from interesting role to interesting role across the Commonwealth, and it's been a fascinating career today.

DAVID PEMBROKE: Do you find working in the APS infinitely fascinating with every day is a new journey, a new opportunity with great responsibility, obviously. You must enjoy it?

HAMISH HANSFORD: I think we have a fascinating job and there's so many challenges out there for society and to be a part of that. At the moment, in cyber security and digital and tech policy, but throughout my career, I think working on issues that actually impact Australians and being at the forefront of some of the great policy thinking in the public service has been both a privilege, but also something that I don't think you get to do in other parts of the economy.

DAVID PEMBROKE: Sure. How do you described that satisfaction though, of being able to work through a problem, work through the solution, seeing it in legislation, then seeing it actually enacted and then seeing the impacts of it?

HAMISH HANSFORD: I think on a day-to-day basis, you often don't pause to celebrate wins, but it's only at points like Christmas, where you look back on the year and say, "Wow, look what I've achieved and look how I've pushed forward a policy agenda or introduced legislation." And I think I'm up to about 20 odd pieces of legislation that I've helped the Government support through the parliament, and you look back and say, "Wow, they're all different and fundamental changes in their own ways to so many different policy problems that impact Australians and Australian lives."

DAVID PEMBROKE: Excellent. Okay. So the next question from the IPAA Future Leaders committee is from Michael Sanese from PWC, and Michael asks, "How have you seen the APS come together to respond to the emerging challenges that recent times have necessitated, particularly relating to cyber security and critical infrastructure? And what are your key learnings from this that we should apply moving forward?"

HAMISH HANSFORD: I think the public service has come together. Last year during COVID-19, we've collaborated in new and different ways, and that's equally true in cyber security and technology policy. I mean, cyber security and particularly technology, is such a defining feature of our society and it's a defining feature of government that, technology, whether or not you're in the tax department or social services thinking about citizens centric technology, whether in home affairs thinking about security and criminality, whether you're in industry trying to promote domestic industry technology issues, or at the very heart of government in a critical tech policy office, or even a diplomat trying to promote technology related issues.

I think that public service comes together on particular new and emerging issues and collaborates in a really productive way. Obviously there's a lot of different perspectives and I think that the great value of the public service is, "How do you have those constructive dialogues, how do you challenge each other?"

And in cyber security and technology I think we do that every day of the year. And from my own perspective, I'm co-located with the operational part of cyber security, so with the Australian Cyber Security Centre. And to have the policy and the operational people co-located, we feed off each other every day. And I think good policy is informed by great operations, and great operations are informed by good policy. So I think the collaboration has been fantastic and something that the public service does well and should do better into the future. And I think technology can be a great enabler of that.

DAVID PEMBROKE: I think that's a key focus really. And I know from the Chief Operating Officer Committee, from the Secretaries Board, it really is a focus on, "How do we bottle the best of 2020 and take it forward? How do we not just revert to the way that perhaps we used to do things?" So what would your advice be as to how the APS can continue to evolve, continue to improve, and continue to collaborate more effectively?

HAMISH HANSFORD: I think we have to continue to break down agency barriers and think about problems. So just like we thought about the supplier of personal protective equipment to frontline officers or Australians during COVID-19, that was the issue. So how do we break down agency barriers and try and use the best of what each agency brings to collaborate on problems and issues. And I think that's the challenge that David Thodey set out in his review about agencies not operating in stovepipes. How do we try and break down those barriers and actually try and support the government and work across agencies. Even when things aren't necessarily in our lane, how do you try and be a great steward of the public service? I think that's the great challenge that 2020 really defined us and we should continue that into the future.

DAVID PEMBROKE: How do you do that though, when you are so busy? I work in many government departments and what I do see is people who are flat to the boards, and with their own jobs, with their own day jobs. And so how do they get the time to think, to be able to go, "Actually, I need to connect with X, Y, and Z, to actually bring a fuller picture to this particular problem."

HAMISH HANSFORD: I think you've got to consciously devote time to networking, to collaborating, to creating the space for a really diverse thought and to try and force yourself in a structural sense. And I think working from home really helps that, because you spend some time in the morning, often without meetings, because you've reduced the commute time. So you can start to structure your day around, "actually that is thinking time and creative time." But you're right, it is a bit of a challenge, particularly in a busy sitting week and with competing demands. But I think you've really got to structure it into your day to make sure that there's time for creative thought.

DAVID PEMBROKE: This podcast, obviously, it's about the public service, and there are many members of the public service who do listen to it. And with those threats that I outlined in the introduction, increasingly it would seem that sophisticated actors are targeting government departments, whether it's in technology or Treasury, as you mentioned earlier. Industry, agriculture, could be anywhere really. How well are we doing as a public service with our cyber security? And what advice do you have to public servants that they could perhaps embrace to ensure that the system of government is robust?

HAMISH HANSFORD: I think the weakest link in cyber security is often an individual. So really being much more conscious about things that are connected to the internet. How do you start to build a culture of security and awareness from every single public servant so people have a deep understanding of how you engage online? The idea in the cyber security strategy of the centralisation of cyber security, potentially through cyber security hubs, I think is also an added way the public service will start to live the ideas in Thodey around aggregation of response particularly in terms of bringing together like-minded groups of people who have the much needed cyber security skills that I know the public sector need and the private sector as well. So aggregation of response, and then really working collaboratively with the Australian Cyber security Centre, I think are all features of how the public service can better respond to cyber security challenges.

DAVID PEMBROKE: So as we sit now, at the beginning of 2021, can you look forward at all and anticipate what may come this year? Or what can you give us as a bit of an insight to the challenges that are coming our way in cyber in 2021?

HAMISH HANSFORD: Predicting the future is often fraught, but 2021 and into the future we'll see cyber criminals be increasingly adept to efforts by law enforcement to frustrate their activities. They'll target vulnerable Australians who have been susceptible to scams, malicious state-based actors will continue to conduct malicious cyber activity. And I think the global environment is one that has pretty significant global competition and cyber security is almost at forefront of one of those great challenges. And you mentioned the Prime Minister and the Defence Minister, in June last year, really said that the issue of the war in the grey zone and a whole range of issues that will really permeate our environment and really challenge Australians in really different ways.

DAVID PEMBROKE: So a single bit of advice to people from here on?

HAMISH HANSFORD: Change your password.

DAVID PEMBROKE: Regularly?

HAMISH HANSFORD: Regularly.

DAVID PEMBROKE: Really? How often should you change your password?

HAMISH HANSFORD: Well, I think the first thing is to make it a unique password. So not a password or something that could be found by a criminal to be easily cracked, but change it regularly. And don't have a single password for every single account that you have, email or bank or whatever it might be.

DAVID PEMBROKE: Okay. All right.

HAMISH HANSFORD: Variety's the spice of life, I guess.

DAVID PEMBROKE: That's very good. Well, I'll get onto that. Hamish, best of luck. You have a very busy job, you have an important job. Stay well, stay healthy. What do you do? Well, you mentioned before you like exercising in the morning, what's your poison?

HAMISH HANSFORD: Well, I went for a bike ride around the lake this morning, and yesterday was a bit of a jog. So between those two, it keeps me busy and I guess lifting up a two year old also it does those arm muscles, doesn't it?

DAVID PEMBROKE: Well done. Okay. Well, thank you for your service and thanks for your contribution and thanks for making time to come to Work with Purpose.

HAMISH HANSFORD: No problem. Thanks so much.

DAVID PEMBROKE: Work with Purpose is part of the GovComms podcast network. And if I may allow myself a moment, the GovComms podcast, which examines everything related to effective communication in government, which is our other podcast, was yesterday rated by a leading Canadian consultancy as one of the top 21 global internal communication podcasts for the second year in a row. And we are indeed in very good company with some outstanding podcasts. So thanks for the recognition and a big thanks to the team and the guests who make that program so special.

Now, the GovComms Institute, which was formed off the back of the outrageously successful GovComms Festival is now up and running and featuring some of the 170 hours of content that was produced by 170 speakers from 20 countries. And a big thanks again to IPAA for their support of that event.

For Work with Purpose, Hamish is the first cab off the rank for 2021, but the team here at IPAA are working hard to put together some of the great personalities from across the public service in coming weeks. If you do see the social media promotion, a like or a share never goes astray, and a review, how we like reviews. So if you do have time, that would be great. So thanks again to IPAA for your ongoing support for Work with Purpose, and also to the Australian Public Service Commission.

DAVID PEMBROKE: Thanks also to the team at contentgroup who are now back at work and helping out our many government clients create more and more content to explain policies, program, services, and regulations, the acceleration of people spending more time online as a result of COVID-19 has certainly upped the ante, but make sure that when you consume that content, you do so responsibly.

So that's it for the first Work with Purpose of 2021, we'll be back at the same time in a fortnight, but for the moment, it's bye for now.

SPEAKER 3: Work with Purpose is a production of contentgroup in partnership with the Institute of Public Administration Australia, and with the support of the Australian Public Service Commission.