INSTITUTE OF
PUBLIC ADMINISTRATION
AUSTRALIA
ACT

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 EVENT

CYBER SECUIRTY IN AUSTRALIA – A TEAM SPORT

ABIGAIL BRADSHAW CSC
Head of the Australian Cyber Security Centre
Australian Signals Directorate

NARELLE DEVINE CSM
Information and Cyber Security Executive
Telstra

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

JUSTINE GOUGH
Assistant Commissioner, Eastern Command
Australian Federal Police

Hosted by **HEATHER COOK,** Deputy Director-General at the Australian Security Intelligence Organisation and IPAA ACT Councillor

6 November 2020

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

HEATHER COOK: Good morning everybody, and welcome. My name's Heather Cook. I'm the Deputy Director-General of the Australian Security Intelligence Organisation, but I'm also an IPAA Councillor and very pleased to be your host today.

Today's session is *Cyber Security in Australia: A Team Sport*, and I'd like to welcome you all here today and know how important it is for us to have these opportunities in this time of COVID to be meeting and have these networking opportunities. Obviously, this event is being run in a COVID-safe way, so I ask you all to assist us in maintaining social distancing and using the hand sanitiser as required.

Can I also acknowledge the guests that are joining us via our online platform, GovTEAMS. I believe we have over 300 who have registered to listen in today, so welcome to those who are joining us online.

Before I begin, can I acknowledge the traditional owners of the land on which we meet, the Ngunnawal people and pay respects to their elders past, present and emergency, and acknowledge their continuing culture and the contribution that they make to life in this city and region.

As I mentioned, we're practicing COVID-safe today. Again, I will keep reminding you about that, but if you're instructed to do something by either the staff here at the National Portrait Gallery or IPAA, just ask that you assist us with that.

It's time to acknowledge our speakers for today, and we have a terrific keynote speaker and a very engaging panel as well. Abigail Bradshaw joins us as our keynote speaker today. She's the head of the Australian Cyber Security Centre within the Australian Signals Directorate. We have Hamish Hansford, First Assistant Secretary of the Department of Home Affairs; Justine Gough, Assistant Commissioner, Eastern Command from the Australian Federal Police, and Narelle Devine, Chief Information Security Officer for Asia Pacific with Telstra. So we'll have an opportunity to welcome our speakers in a moment.

So the event today, Abigail will join us and outline her priorities for the Australian Cyber Security Centre on the back of the government's release of the Cyber Security Strategy 2020, which was released in August of this year. We'll also be discussing how government, industry, and the community can work together during a time of emerging cyber threats and a global pandemic, to ensure a more secure online world for all Australians.

There's no doubt that our society, our communities, the global environment is increasingly dependent on the cyber backbone that enables it. It's hard to imagine 30 years ago, the extent to which the movement of money, information, and people on such a scale and magnitude would exist. Every aspect of our society is now linked and dependent on computers or the internet in some way. It's enriched our society in many ways, it's created huge opportunities and efficiencies, but it's also created vulnerabilities as well.

So short of turning the thing off, which I know at least at a minimum would send my kids into some sort of withdrawal, what do we do to operate safely in this cyber-connected world? That's what we're going to discuss today.

Format will be Abi's keynote address. Then we'll ask the panel to join us on stage. We'll hear from them on their issues. And then we will open for a Q&A. Today's event is going to be live streamed. So it's being recorded and will be made available to view online as part of the post event resources page.

So without further ado, it's my pleasure to introduce our keynote speaker, Abigail Bradshaw. Abi began her career in the Royal Australian Navy before transferring to the Department of Home Affairs for senior offshore roles, covering Europe and Sub-Saharan Africa. She was also the inaugural chief risk officer. Abi then transferred to the Department of Prime Minister and Cabinet as the head of National Security division prior to becoming the deputy coordinator of the National Bushfire Recovery Agency. Abi was awarded the Conspicuous Service Cross in 2005 and holds a Bachelor of Laws as well as a Bachelor of Asian Studies. Please join me in welcoming Abi to the stage.

ABIGAIL BRADSHAW: Well, good morning everybody. It's so nice to be with people. I was saying to Caroline Walsh this morning, I spend hours talking to people from this little, tiny room that we've set up with beautiful screens like this, and sometimes you never know who's on the other end. It's a wonderful feeling actually, just to stand in front of humans and talk to humans, and particularly a grouping of them. It feels kind of illicit, but actually quite nice.

I want to acknowledge the Ngunnawal people and the Traditional Owners of the land on which we meet today. I want to pay my respects to elders past and present and emerging. And I want to acknowledge their ongoing and continuing rich contribution to our land, waters and culture.

And this is especially important on the eve of NAIDOC week, when we will celebrate that the Aboriginal and Torres Strait Islander people were Australia's first explorers, our first navigators, our first engineers, our first farmers, our first botanists, our first scientists, our first diplomats, our first astronomers and our first artists.

Always was – always will be.

I'd like to thank IPAA for welcoming the Australian Signals Directorate's Australian Cyber Security Centre again to this excellent forum, and for the opportunity to speak about our really important cyber mission.

Our secure connectivity has been critical to maintaining our lives through COVID and it will be equally critical to facilitating our pathway to economic recovery.

I also want to thank this excellent panel for joining today's discussion. There's something special about today's panel, and I'll include Hamish in this remark. It's full of fine women. Including our moderator. And that's a really outstanding position to be in, in a field which isn't always dominated by our gender. Collectively we represent a core component of 'Team Australia' – the combination of government policy, operational and law enforcement, and importantly industry capabilities, which are representative of the teamwork necessary to achieve our ambitious objective of making Australia the most secure place to connect online.

More broadly, I want to acknowledge other critical members of Team Australia in this room and online today. The ubiquitous nature of cyber means we all have a role, so I want to call out a few examples of the close collaboration we have enjoyed:

With DTA, in ensuring cyber security by design informs government digital services and architecture.

With Services Australia, in the delivery of government services hardened against prosecution from cyber criminals.

With the ACCC, the e-Safety Commissioner and the Australian Information Commissioner, all of whom we work closely with to ensure Australians hear one voice – one strong singular voice and message - on how to mitigate the impact of online harms, scams and preserve digital privacy.

With DFAT, who advance our global interests through diplomacy on cyber norms and standards offshore, and

With the Department of Health, who have worked with us to ensure our advice and assistance reaches health providers most vulnerable to cyber attacks during the pandemic, and ensure that our most important health supply chains are best prepared for future challenges.

And I also want to acknowledge the Australian people as part of that partnership, who have inundated us with their curiosity and seeking advice over the last 12 months, increasing our call load by over 200 per cent in their aim to lift Australia's defences against malicious cyber actors.

The ACSC cannot and does not prosecute its function without partners. It will take a broad church, and an even broader Team Australia, to achieve our mission. Emphatically, and perhaps obviously, that 'team' theme will remain central to our panel discussion today and our efforts into the future.

Recognising the rich history on the walls of this building, and the way they remind and speak to us of Australia's past and future, I'm just going take a moment to reflect on how we got here.

ASD's cyber security function is as old as ASD itself – in fact, we're 73 years old on 1 April 2020. That's not a joke. It's just the way it is. ASD's first incarnation, the Defence Signals Bureau, opened in 1947. It was responsible for exploiting communications and for communications security in the armed forces and government departments.

The Australian Cyber Security Centre, evolved from this history, through the 'Q Branch' or information security branch. The 'Q' of course, stood for 'quartermaster' or the keeper of the keys - the term given to generating the cryptographic material that encrypts our government and military communications to keep them safe. It's a vital role which we still play today.

The Q Branch also performed our communications security role.

This coupling of exploitation and defence – or poacher and gamekeeper – is as useful today – and possibly even more critical – than it was even back then.

Our 'protect and assist' function continues to be enriched and informed by our insights into the motivation and intent of our adversaries, and the techniques used to successfully exploit foreign communication systems.

The next substantial evolution of our cyber security function occurred in 2010, when the ASD stood up the Cyber Security Operations Centre, or CSOC. In November 2014, the CSOC further evolved into the Australian Cyber Security Centre.

The 2016 Cyber Security Strategy recognised the rising threat and scale of malicious cyber activity, as well as the importance of cyber security and resilience for innovation, global connectedness, domestic prosperity and unity.

The strategy initiated the process of collocating all government operational capabilities into the Australian Cyber Security Centre. By 2018, the ACSC was joined and enriched by the Computer Emergency Response Team from AGD and cyber security staff from the DTA.

Joint Cyber Security Centres in Sydney, Melbourne, Brisbane, Adelaide and Perth were opened, reflecting the importance of strong collaboration and partnership with industry and community.

And the ACSC gained an expanded remit for providing technical advice and assistance to governments, to the private sector – big and small business, critical infrastructure, families and individuals.

An expanded 24/7 response team was stood up to service our customers. And, in amendments to the Intelligence Services Act in 2018, ASD gained powers to prevent and disrupt cybercrime undertaken offshore.

The 2020 Cyber Security Strategy builds on the strong foundations of the 2016 strategy, on the strong and capable leadership of my predecessors, and on our even longer history of providing excellent cyber security advice and assistance.

Like the 2016 strategy, the 2020 strategy continues to emphasise the shared responsibility for cyber security for community, industry and for government, and the criticality of close partnerships to realise our shared objective.

It's with this context that I want to talk about going forward. The cyber landscape has evolved. It's escalated and it's expanded quite significantly. It is indisputable that the scale, frequency and sophistication of malicious cyber activity is on the rise.

Professionally organised and transnational cyber criminals, as well as state-based actors, are exploiting vulnerabilities and developing viruses, Trojans and more sophisticated ransomware for the purpose of stealing money and sensitive data.

New technologies like the Internet of Things will bring tremendous benefits. But they will increase the threat surface that our adversaries will seek to exploit. By 2030 an estimated 21 billion devices are expected to be connected to the global internet, with some estimating an eye-popping 64 billion by 2035.

Since the pandemic onset more than six months ago, the ACSC has observed a sharp rise in email phishing, message scams and ransomware attacks targeting COVID-19 services and stimulus and welfare programs.

Cyber criminals have demonstrated organised and informed capability to amend their scams to align with government assistance schemes, tailoring them really quickly with their lures to resemble messages from those we trust – like government welfare or health providers.

Over the last financial year our Report Cyber reporting tool received almost 60,000 cybercrime reports. That's about one report every 10 minutes and each one of those was worth on average about $5,000.

Over the same period, we have observed sophisticated state-based actors targeting all levels of government, private organisations and industry.

Globally we have seen a rise in devastating ransomware attacks on businesses and services, and attacks on critical infrastructure, including devastating disruption to energy and health services.

The costs of these malicious activities are grave. There are the obvious financial costs of lost revenue and business, the loss of market position, opportunity and strategic advantage that arises from the theft of IP or sensitive commercial information.

The loss of amenities and essential services and privacy is real. Less obvious – but equally significant – is the potential to undermine the confidence of Australians to live life and prosper through digital means.

It's why what we do now as Team Australia really matters.

This context has informed the 2020 Cyber Security Strategy. The vision of that strategy is 'a more secure online world for Australians, their businesses and the essential services upon which we all depend.

Consistent with that vision and emphasis, the strategy is underpinned by the government's investment of $1.35 billion in ASD's Cyber Enhanced Situational Awareness and Response – or CESAR – package.

Speed, scale, volume and impact – and wherever possible achieving this through automation and machine speed – have all been objectives of my predecessors. They remain as relevant today as they have ever been. The operational investment in CESAR will assist us in achieving that goal.

So what is CESAR and what will it do for you?

The key components of CESAR that we will bring to life over the next decade include:

- A new partner portal coupled with a multi-directional threat-sharing platform. This will enable us to share indicators of compromise at speed and scale, and in machine-readable format, with all out partners. Importantly, the multi-directional capability will enable our holdings to be enriched by the insights of business, industry and our partners.
- We will expand and uplift our Joint Cyber Security Centres all throughout Australia, improving their capacity to receive and share classified information.

- We will roll out a national exercise program, expanded, focussing on our partners in critical infrastructure and ensuring that we are ready to respond when our worst cyber day happens.
- We will extend and expand our offshore cybercrime disruption, continuing to work closely with our law enforcement partners, and establish a countering foreign cybercrime capability within the ACSC.
- We will employ and progress technologies that block threats automatically – partnering with industry to mitigate at scale – like our protective DNS system that will enable partners to automatically block a range of malicious content, with the effort of a couple of lines of code.
- We will expand our customer engagement channels, extending our 24/7 cyber security help desk to service the needs of small business and families.
- We will develop and enhance our awareness and education communication, working with our government partners to ensure Australians have access to a singular authoritative and trusted government voice on cyber security.
- We will continue to bolster cyber resilience, particularly with critical infrastructure and government, through our uplift, Cyber Hygiene Improvement Program and vulnerabilities assessment services.
- Collectively, we will leverage our partnerships with federal, state and territory governments, with critical infrastructure providers and industry, to build a national situational awareness capability that we are able to share at speed, scale and, wherever possible, automatically, to assist in the protection of all Australians.
- And where entities are unable to mitigate threats, we will continue to deploy incident response capabilities and specialists to assist.

CESAR is not an investment in ASD or ACSC alone. The operational capability will belong to all Australians, available to defend, assist and to uplift the cyber resilience of government agencies, Australian businesses and communities.

Importantly – it will assist us to make our collaboration with the AFP and the ACIC more potent, impactful and frequent.

Together with ACIC and AFP this year, we have used our collective capabilities to successfully disrupt the business model of key foreign cybercrime syndicates targeting Australians through COVID-19-themed SMS phishing campaigns.

In doing so, we protected hundreds of Australian and thousands more foreigners from organised and sophisticated foreign cyber criminals.

Under the 2020 Cyber Security Strategy, and with the benefits of the operational investment in CESAR, we seek to replicate our recent exemplar partnership with Telstra and Services Australia which successfully identified and rejected illegitimate phishing text messages that are impersonating myGov and Centrelink, before they reach Telstra customers. This partnership pilot demonstrates how government and industry can work together better to protect Australians from cyber threats.

And knowing there are so many more valuable insights and examples my panel colleagues will share – I'm going to leave it there and I look forward to the panel discussion.

HEATHER COOK: Thank you very much, Abi, for that incredibly informative speech. I'm going to now invite our panel members to join us on stage, and as they do so I'll give a brief introduction and biograph on each of them.

Hamish Hansford is, as I mentioned before, the First Assistant Secretary of Cyber, Digital, and Technology Policy at the Department of Home Affairs, and was previously also the first assistant secretary of National Security and Law Enforcement Policy. Hamish has held multiple senior executive positions within the Department of Immigration and Border Protection, and the former Australian Crime Commission. He's also served in a range of intelligence, policy, planning and program delivery roles in the Department of Prime Minister and Cabinet, the Attorney General's Department, the Australian Senate, and the Office of Transport Security. Welcome, Hamish, to the panel.

Justine Gough joins us. Justine is the Assistant Commissioner of the Eastern Command in the Australian Federal Police, a position she was appointed to in February of this year. Justine started her career in the AFP in 1990 and has worked in a variety of portfolios, including organised crime, counter terrorism, political and sensitive investigations, intelligence, and child protection. She was also posted to Hong Kong in 2015 as the AFP Senior Liaison Officer with area of responsibility for Hong Kong, Macau, Taiwan, South Korea, and Japan. Justine holds a master's degree in Psychology and Terrorism, Safety and Security, and has a Graduate Diploma in Dispute Resolution.

Narelle Devine joins us. Narelle was appointed to the role of Chief Information Security Officer Asia Pacific in Telstra in July of this year, a role that she also previously held in Services Australia since 2006. Narelle began her career at the Royal Australian Navy as a commander with focus on communications, electronic warfare, and cyber operations. Narelle was also awarded a Conspicuous Service Medal in 2006. She also holds a Masters of Systems Engineering, Masters of Science, and a Bachelor of Arts, all from the University of New South Wales. Welcome to you all.

So we thought we would start with a bit of a discussion and perhaps build on Abi's speech before we open up to questions in the audience. I might invite each of the panel members to perhaps spend about five minutes giving us or sharing with us a brief reflection from their perspective on this issue. Hamish, would you like to start?

HAMISH HANSFORD: Sure. Well, thanks very much. Abi, it looks like the Australian Cyber Security Centre is having a busy operational year and lots of work ahead, particularly with us and from a policy perspective. And it's been a big policy year for cyber security, and it's been 2,233 hours since the Cyber Security Strategy was launched on the 6th of August, or 93 days. So 93 days into implementation.

I thought given the threat that Abi's outlined and the context from 2016, the strategy that really set out the building blocks, I really wanted to give you a sense of the big idea in the 2020 Cyber Security Strategy, and give you a sense about how far we've progressed and what are the next steps.

So 2020, based on the threat that Abi outlined, the government really put forward the protection of our critical infrastructure as a key part of not only the Cyber Security Strategy in 2020. And there's a lot in the strategy ranging across a whole range of fields of endeavour, and particularly partnerships with industry and individuals in the community. But the big idea the government wanted us to focus on is how do you protect critical infrastructure? How do you define the sectors that are really, truly critical to the functioning of our society and our economy?

There's 11 sectors that we've outlined in a paper that the government put out on the 12th of August and started to consult industry. Eleven sectors which are critical to the functioning of our economy. I think if COVID-19 has really taught us anything, expect the unexpected. The different sectors that are really critical for our economy, we've been engaging with over the last 80 odd days, and we've met 2000 people. We've had close to 200 submissions to that discussion paper on the 12th of August, which really set out, how do we try and protect our critical infrastructure across each of those sectors?

Under underpinning that, we've tried to define… Well, what is critical infrastructure, and what are the critical infrastructure assets which are truly critical to the functioning of society, to the functioning of our security, and underpinning our prosperity and digital future? How do you then go about protecting them? We've looked at consulting with industry on, well, what does it really mean to protect the critical infrastructure asset from a cyber security perspective, that Abi's spoken about today, but also from a supply chain perspective, from a physical security perspective, and then a personnel security perspective? How do you apply that to critical infrastructure assets, which are really, really critical to our functioning?

Then, in addition to that, well, there are some systems, which are so critical to the functioning of our society that, if they were subject to a cyberattack, they would have a detrimental impact on how Australia functions. You look at the nightmare scenarios of a cybercriminal or a threat actor taking over our air traffic control system, shutting down a power plant, or some of those nightmare scenarios. For those systems of national significance, which are really truly interconnected and really would have a detrimental impact to our society, how do you put additional cyber security protections on those assets, and how do you have a better collaborative relationship, particularly with the Australian Cyber Security Centre? It's the broad frame of what the government's trying to do in uplifting our cyber security, and physical security, and personnel security, and supply chain security around our critical infrastructure assets.

The government will shortly release exposure draft legislation, which, again, builds on the theme of today that cyber security is a team sport and we are looking to consult with industry, in particular about, how do we build the best regime possible so that everyone in Australia feels more secure, through a more secure critical infrastructure sector? Of course, government is a part of the functioning of our society. Another big theme in the cyber security strategy is, well, how do you try and make sure that government uplifts that cyber security in and of itself? Work is underway, particularly through the Secretaries Digital Committee in the Commonwealth level to try and uplift our own cyber security and making sure that, how do we build aggregation of response, particularly through sharing of information, sharing of skills, and sharing of capability to have a better response to cyber security at the Commonwealth level? That's really how that the Australian government, in particular, fits in with the overarching principles of critical infrastructure and what the government's co-designing with industry.

The big idea that I think really links closely with all of the operational issues that Abi mentioned about better connectivity with industry, trying to build a regime from a policy perspective about, how do you uplift our own security across some of those really key parts of our economy? That's the big idea. There's a lot in the strategy, and we're on track for implementation across a whole range of different areas, but I thought, in particular, I'd highlight that point that we're working on at the moment, Heather.

HEATHER COOK: Thanks very much, Hamish. Justine.

JUSTINE GOUGH: Thank you very much, Heather. Hello to everyone. Thank you, Abi, for your address, and certainly do concur with your points about some cyber being such a team sport, which is certainly, from my agency's perspective, something that we are adopting and will be focusing upon into the future.

Against the backdrop that Abi has described, it's no surprise that in 2020, the Australian Federal Police elevated cybercrime amongst its top five criminal investigation priorities. In that environment, cyber has such an influence in relation to those other crime priorities. A lot of the crimes that we see are cyber-enabled. So counter-terrorism, foreign interference, financial crime, transnational serious organised crime, and child exploitation all have cyber elements and are in touch, in some way, from cyber-enabled criminal activity. The AFP is focused upon those types of elements of cyber-enabled crime. But it's also very focused on, I suppose, traditional cyber-related criminal activity, some of which Abi has described today, everything in terms of significant computer intrusions, hacktivism, distributed denial of service attacks, and ransomware.

But in relation to the environment that Abi describes, it's not, I suppose, the attacks on governance and government systems, critical infrastructure, et cetera. It's the effects on mums and dads across Australia. Into the future, I think that this is an area of extreme partnership between the AFP and our states and territories, particularly in relation to the volume of reports that are coming through in Report Cyber and the very large and real impacts on everyday Australians of cyber-related criminal activity. As part of the Cyber 2020 Strategy, the AFP has been provided with funding of $88.9 million over four years. This relates to the environment that is described. The fact that criminal activity takes place and is enabled via dark web, via... I can never say that word, anonymizing technology. These present some challenges in terms of law enforcement, challenges of identifying those responsible, challenges of apprehending, and bringing those who are perpetrating criminal activities to justice.

The funding will enable the AFP to recruit a hundred new offices, investigators, technical specialists, intelligence offices. That will bolster our activities in terms of working in a really, really collaborative fashion and a very dedicated way of combating these activities and the threats posed to everyday Australians into the future. The AFP will work very hand in glove with the ACSC, with the ACIC, and a variety of other agencies, as well as with industry, in terms of its activities in arrest and prosecution, and also supportive of the prevention activities of the ACIC and other elements that Abi has mentioned today. Because prevention and education, I think, is our greatest tool and an opportunity that we can arm everyday Australians with the skills and the tools and the knowledge that they need to prevent the perils that are posed by the activities posed by cybercrime into the future. Thank you, Heather.

HEATHER COOK: Thanks, Justine. Narelle.

NARELLE DEVINE: Thanks. Good morning, everybody. I think I'm probably in a really fortunate position to have been able to live both sides of the fence now, and certainly on this side only for a really short period of time so far. But getting to look at Services Australia and being CISO there, and seeing the impact of the cyber operations, and how they grew that capability, and how they understood how important that was, and how they plugged into government and watching the development of the cyber security strategy over the last few years with government eyes, it's now lovely to sit on the other side and be able to contribute so much to both of those plans, and to be able to link in to all of the agencies, particularly the AFP and ACSC and ASD in order to help and provide those services.

Moving to Telstra was fabulous. They have this amazing visibility, and there is all these other things that go on that you can actually do good. It's been great to be able to link back in. Whenever I'm talking about it being a team sport, truly it is a team sport. As CISO, literally, I stopped being Services Australia and changed to Telstra. All that changed was the company name at the end of my title. The group that I talked to, the people that I interact with every day, they're all the same. It's the same problems, the same threats, the same issues. It's no different.

The great thing about being in industry is that we span such a huge remit. We can impact government, but we can impact all the way down to those small businesses, the moms and dads, we get that reach, and we're able to influence in a way that's really unique. For us, it's really important to stay engaged and stay for that combined, that single message, and make sure that we're on message. We're delivering that same level of awareness and education through every customer that we have and make sure we're doing our part to uplift cyber for the country as well.

HEATHER COOK: Thanks very much, Narelle. Thanks to the panel for sharing those reflections. Just listening to those reflections and certainly drawing on Abi's speech, the shared responsibility theme is common throughout and critical to success in this area, obviously. What are some of the challenges associated with engaging community, engaging broader industry, or the private sector on these important issues? What are some of the challenges? Perhaps: how does the strategy propose initiatives to address some of those challenges? That'd be for anyone to start. Abi, if you...

ABIGAIL BRADSHAW: I'll speak from a technical perspective and my learned experience of the last eight months in the ACSC. It would be wrong to say that there wasn't a partnership and in the past because there always has been. Is my mic working now, because I can hear myself loudly? But-

HEATHER COOK: I'm not sure it is.

ABIGAIL BRADSHAW: I was sitting on it. There we go. How's that? Happens with the remote at home, too, and the channels are changing. What I was saying was it would be wrong to suggest that there hadn't been a level of collaboration and partnership in the past. There always has been, and that's growing exponentially. I think, though, what confronts us now is the scale, particularly as the threat surfaces - I tried to explain - has expanded so exponentially, and the speed, of course, that the threat arises. The issue is, actually, how do you get that information in a usable format to people who have a variety of different levels of needs and competencies?

We've spent quite a bit of time this year in the ACSC focusing on our customers. There's only 20 million of them, and, obviously, all with varying needs. The needs, for example, of a critical infrastructure provider, who has complex OT, are going to be entirely different to a family that's just trying to conduct their lives on a day-to-day basis from home. But our objective is to make sure that the advice that we do provide is in the most practicable format dependent on audience. By way of example, on the 19th of June, we issued a, what was described as, copy and paste advisory, which addressed the vulnerabilities which the prime minister and the minister spoke about that morning, the sophisticated state-based actor and the particular vulnerabilities that that actor was using.

In the front of that piece of advice, we gave some pretty practical advice about patching your system, about having backups, et cetera. In the back of that advice and linked to it were a sequence of technical, what we call, indicators of compromise, which would mean nothing to a family but would mean something entirely different to someone like Narelle.

What we know is that that advisory was downloaded about 300,000 times in the first days, following the prime minister and minister's statement, which is an awesome thing for us. It means, on one level, we're getting our product out. That's KPI number one. But how do we actually know that people are absorbing that in a useful way?

Well, the KPI, for us, was the number of calls we took as a follow-up, as a consequence of the alert that had been raised and the awareness had been raised. The number of people calling us who were actually in a position to be able to say, "We used your indicators of compromise, and we think we've got a problem," or, "We think we're okay." That's the more important KPI for us. It's the one that we will strive to continue to assess going forward.

It's not just about reach. It's about how practical that advice is. That's the challenge. That's the example of the challenge. The opportunity for us goes to the funding under CESAR to facilitate that multi-directional sharing platform.

In the instance of the copy and paste advisory, what that meant was that those that had the technical competence to understand those indicators of compromise had to sit there, manually typing them in. With our multi-directional sharing platform, that advice will be pushed out in an automatic way at machine speed and at scale to everyone who's registered on our customer reference system, which is wonderful. That's a massive step up for us. But more importantly, the multi-directional element of that will mean that people will be able to read it, see it. Excellent people like Narelle, who have that enhanced visibility, will be able to build on our initial assessment of those indicators of compromise, enrich them, send them back to us so that we can start that cycle all over again.

HAMISH HANSFORD: Thanks, Abi. I think great question because industry collaboration, and collaboration more generally, is really critical to any response to cyber security. I think the Prime Minister, when he announced the cyber security strategy on the 6th of August, said that the key ingredient is you. I think he was really talking to all Australians and putting a call out to uplift all of our own cyber security.

I did mention the collaborative work we're doing on critical infrastructure. One of the other initiatives in the strategy is setting up an industry advisory committee. It's great to have an Industry Advisory Committee member here in the audience today, in Rachel Falk, but Andy Penn chairs the government's Industry Advisory Committee. That's a great way to bench test a whole range of different ideas as we mature the strategy implementation and bench test every policy idea that goes to the government starting from critical infrastructure.

That's one answer. If you look at the strategy in paragraph 66, the government announced a best practice regulation task force. I think that really epitomises the need for collaboration and working together on cyber security because that really talks about: How do you uplift cyber security across the rest of the economy? While the government's focused initially on critical infrastructure, how do you try and uplift all Australian cyber security?

That is a diverse policy issue as privacy issues and looking at the Privacy Act, to the Consumer Data Rights, to working out how do you use nudge and behavioural theory to uplift cyber security, to looking at about how do you convince bigger enterprise to put packages of services for smaller to medium enterprises, and how do you get education and awareness campaigns. Really, a whole package of issues that require any form of consultation and, more importantly, any collaboration is required to be successful. I think that the strategy has a whole range of initiatives that are premised on the fact that collaboration is critical. There's a man right outside the window trying to balance on a beam. It's a big balancing act for cyber security as well.

HEATHER COOK: There is all of that emphasis and there is a significant amount of money being invested in this area. I'm quite certain I know the answer to this question, but how do we continue to tackle complacency? Does it take crisis or major compromises or loss, a theft of identity, or some issue, before we're actually getting the attention to this issue that we need so that it is a shared responsibility? Justine, do you have some thoughts on general complacency around this issue?

JUSTINE GOUGH: Well, I probably would observe that COVID has been, certainly, a situation that's challenged us all. But I think it's probably forced some access from an everyday Australian perspective to the fact that you need to actually use a QR code to go to a cafe and things of that nature. I think that a lot of the dialogue, a lot of the discourse, is about we are in a digital economy. I think that perhaps we are in a little bit of a cusp. Complacency is always a thing that we do need to deal with. But, I mean, I think that the world has changed quite considerably with regard to COVID. Obviously, there's been a lot of challenges along the way, but maybe it's been a bit of a turning shift for us that we do need to be a little bit more digitally aligned, and perhaps that's a good situation that we can build on into the future.

HEATHER COOK: Narelle, I'm wondering if you could perhaps share with us what you think the ideal vision for government-industry cyber partnership looks like, perhaps over the next two to three years? What would good look like in this area?

NARELLE DEVINE: I think we're really getting there. I think we're getting to what good looks like. We've had a really large journey over the last few years to build all of that. But good looks like that we're just interconnected. We share openly. We share easily. We get the legislation right so that we can. We get the relationships right so that we can, and we're able to do so in a way that's really beneficial to everybody. As I said, we've made huge roads towards that. I think we've got a tiny way to go, but not that far. The relationships are there. The sharing is there. It just needs to, now, expand. I think all of the work that Abi and the team are doing in CESAR is going to expand that. The strategy certainly supports that. I think we're set up for success. It's now on us to deliver.

HEATHER COOK: Very good. Thanks for that. Hamish, how has the strategy been received? Has there been a sense of uptake or interest in it that you can account for?

HAMISH HANSFORD: Sure. We were pretty surprised that 9,000 individuals downloaded the strategy themselves, in addition to the reporting in the media and advertising from government in the sense of public statements. But pretty broad approval from a range of different stakeholders, we think, has been received. I think that the really important thing that proceeded the strategy was a really detailed industry advisory panel report, which set out 60 recommendations for the government to consider, which covered all forms of cyber security. The strategy then followed the approach of responding to that report, which was really based on industry consultation, industry engagement, and part of that deep engagement by the government, through the Department of Home Affairs, 1400 individual individuals spoken to 214 submissions. I think on the back of all of that industry, and academic, and individual consultation, and industry advisory panel report. Then, really trying to pick up some of the big issues and crisply and very succinctly trying to articulate it in terms of what the government will do, what industry is expected to contribute, and what individuals are expected to contribute. I think that package of both consultation and the way it was delivered, I think, has got pretty broad agreement, not only domestically, but internationally as well. Hopefully, that's the case, and hopefully, that continues.

HEATHER COOK: That's great. Maybe for our operational agencies, for Abi and Justine, both of you commented on the ubiquitous nature of the conductivity and that cyber backbone. The transnational nature of some of the crimes that we're dealing with. Clearly, the end-to-end point of computers and the internet doesn't mean everything's happening within the boundaries or the borders of our own country. How are we engaging internationally on this issue, and how challenging is countering the threat of a cyber threat when that threat is so global in nature?

ABIGAIL BRADSHAW: Yeah, sure. Just let me check if I'm sitting on [the mike] again. As I mentioned earlier, the benefit of the ACSC sitting within the ASD is that we've got 75 years of history of Five Eye relationship trusted and close through classified systems that operate. Actually, for me, it's much easier for me to talk to my Five Eye counterparts on a classified system at the touch of a button than sometimes it is to connect on a WebEx. We're so much better classified than we are in... Anyway, we are getting better at that. We've had to because of COVID. That real-life, 24/7, around the sun, interaction happens in abundance at all levels, from the Director-General... Well, in fact, beyond that. From the ministerial level, through to the director level, at my level, with my US, UK, Canadian, New Zealand counterparts on a regular basis, despite COVID, and then on a continuous basis through the actual technical experts who are doing the work.

There are too many to count instances where either we have discovered a vulnerability and pushed it out to our international counterparts to their benefit, because we've seen it first. That's the benefit of having those long traditional, Five Eye relationships because cyber is global. And quite often, our capacity to prevent is informed by those who've seen it first, and quite often that happens offshore. The other aspect, and great example I would say, is ransomware, for which of course there isn't just one type. There are multiple variants and the capacity for us to partner offshore with those, particularly law enforcement agencies. Even in the EU, there's been a Centre set up that solely focuses on pulling apart different variants of ransomware and then sharing the results, so that we're capable of collectively developing the tools that will assist Australians in the event that they're attacked. So, really important, Heather.

JUSTINE GOUGH: Thank you, Abi. And certainly, would absolutely agree in the law enforcement space there's collaboration at the Five Eyes working group level with regard to cybercrime and collaboration on those specific themes, but also strong connections with Interpol, with Europol. And in addition to that, the AFP has three dedicated cyber officers who work in overseas locations, and the funding will enable us to increase our network to six in strategic locations, so parts of the world where specific threats emanate, and we will have offices on the ground to work with local authorities to work specifically to combat these types of crimes and the impact that they have on everyday Australians.

HEATHER COOK: Thanks Justine. Narelle, I'm never aware of Telstra's Cleaner Pipes initiative. I'm wondering if you could perhaps share with us what that program is about and what success it's enjoyed, and perhaps what the next steps might be?

NARELLE DEVINE: Yeah, absolutely. So, Cleaner Pipes in a nutshell is about making it safer, so about making the Internet safer, our telephone calls safer, the SMSs safer. The first component to that is DNS scrubbing and we're looking at really look at the infrastructure behind that, so how can we stop bad things coming to you to start with? And then, how can we scale that? It's one thing to do it once or twice or to do it as point solutions, but most of you out there will understand cyber's a bit like whack-a-mole, if you try and do it like that, you're just chasing your tail. We're looking at solutions that enable us to have big impacts, so stop one thing and make the benefit for many.

The most recent part to that is that SMS sender ID blocking and that was a partnership that we have now with Services Australia. We initially tried it on ourselves first, obviously, made sure it worked; but coming from Services Australia, the impact that those militia or the false/the fake SMSs, MyGov, Centrelink, et cetera, have on those Australians. You are using those services at a time of need. The last thing you actually need is for someone to impersonate those services and to trick you into giving away identity information or even money, et cetera, so I think the ability for us to actually start to have an impact in that space is amazing.

We know where things come from; we know where they go. We're able to have an impact there and we're able to stop those fake SMSs getting to our customers. The plan obviously, again, is to be able to scale that and to be able to do even more, and we're looking at where that goes next, which are the next highest misused SMSs, if that makes sense, and target the activities to where they'll have the greatest impact for the overall community.

And then, there's a number of other initiatives following on from that around the URLs, just making the email safer, getting rid of scam phone calls themselves, all of those types of initiatives that are coming. So, this space is going to be really exciting over the next 12 to 18 months as we not only start to execute those, but we're able to scale them to a degree where they actually have this amazing impact on the Australian community.

HEATHER COOK: Thanks very much, Narelle. A number of you, and certainly Abi in particular, mentioned the impact of COVID, the pandemic, on this issue and so many other aspects of our lives. But I'm wondering if we could hear a little bit more about how that has impacted on the cyber threat, how quickly both are foreign actors and criminal networks have seized on some of the opportunities that have presented?

It's an area where I think, just more broadly, it's difficult to stay one step ahead of the bad guys. Can you just describe a little bit more perhaps about how that threat has manifested and whether we see that as a persistent issue that we really need to get ahead of, or whether we're keeping up with that?

ABIGAIL BRADSHAW: Sure. I guess there's two main issues that arose out of COVID for us that changed the way that malicious actors could go about getting at Australians. There are so many more people were working from home or remotely. What that means is quite often people working from home might not be using devices, and so they might not have the same protections that a corporate device might have. Perhaps they're older; perhaps they're not patched as regularly, so that'll create a new threat.

The second – and we see this regularly if you analyse the report cyber data, which we've now got for just over 12 months – is that there is a pattern of cybercrime, which follows whatever is socially current. I saw it when I was at the National Bushfire Recovery Agency. Criminals quickly pivoted their scam to bush fire recovery welfare payments, by way of example. We see it around Christmas time with post and parcels become a target for cyber criminals. But the most incredible observation, I would say, through COVID is how quickly and well-organised and well-educated those cyber criminals were on Australian policy settings.

We observed cyber criminals adjusting their techniques and their lures within hours of the announcement of an Australian welfare policy service or information system, so that's the scary part, I suppose. And that's why our collaboration with the AFP, but also with those in government who are charged with providing those services and the facilitators of those services like Telstra (is so important). And in fact, the big signal here through the cyber security strategies, in fact, is how special in the future relationships with industry like the telcos will become. Because, as Narelle said, their level of visibility, their access to enormous sizable traffic, means they are best postured to see what looks strange and what looks abnormal.

And so, that's why in order to get ahead of those, that incredibly well professionally organised, incredibly well-informed syndicate criminal syndicates, we need to work collectively with those in government that are providing the services to ensure that they are cyber Secure by Design, so they're hardened to the full extent possible; and that those that are responsible for managing the traffic and have great visibility of the traffic, are able to either block it from the outset, or at least tell us when they think something's going wrong.

JUSTINE GOUGH: I think that... and we see this from an AFP perspective in the drug space... Australia is quite a lucrative market. And I think from a certainly financial fraud and scamming perspective, Australia has been seen as a target of criminal groups are incredibly able to pivot, to change to network and that presents such a challenge for us collectively as agencies. We need to ensure that our technologies are where they need to be, our tools, our techniques, our skills of our officers: our people who are employed in our agencies.

You mention whack-a-mole. It's that one step ahead. There's a notch that's increased in terms of pivoting and changing, and certainly, that's always a challenge collectively for us as agencies. I think that our adversaries will always look for opportunities to exploit those vulnerabilities, to exploit those opportunities, and we need to actually ensure that we can quickly pivot and adjust in terms of our ability to work collectively and to focus on the new challenge that exists.

NARELLE DEVINE: We've certainly seen that change and I think for us, internally, we've even put a focus on that, so we always had people that interacted with ACSC and Home Affairs and law enforcement. We've now actually, in the last few months, just put them all into one team under a national security banner. And then, there's a focal point within my team. It's a team in their own right that just does this day in day out because it is becoming so critical we're interlocked in the best fashion we can be.

HEATHER COOK: Thanks very much for that. So, we're going to move to some Q and A, so while you're all thinking of your questions, and before I throw to our audience present in the room today, I might start with a question that's been submitted by one of our online guests. So, Kristin Barrett from the Department of Finance asks the following question: "Intelligence sharing and collaboration across government is critical, yet enterprise IT plans are generally not interconnected, and easy to use apps like Zoom invite a range of cyber security issues. How can the Public Service achieve a collective solution for secure across government collaboration?" Very good question. Anyone like to have a crack?

ABIGAIL BRADSHAW: Do you want me to start from an operational perspective? What a great question from the Department of Finance. They always have the best questions, don't they? So, I'm just going to start with a statement of fact and that is that the public service, although it may look like to those outside of Canberra, one homogenous service, actually isn't. That is because of the enormous range of services that are provided by the public service.

So we have agencies that are... and with no examples, of course, in mind... but quite introspect and are able to operate quite autonomously who might have quite simple IT needs, in the sense that, without being pejorative, perhaps they're a policy agency whose IT needs aren't as complex as say, Services Australia, who has to provide a huge amount of interaction with the Australian community or, for example, run a global visa system in which we have to because of the size of people who, well, used to visit Australia at least, and our migration program, and the complexity and the need for us to manage that securely and connect it with other systems that do checking and vetting, and so on, and so forth, have much different requirements.

The other point is that they don't all start at the same standpoint, i.e., some have large legacy systems, some have new systems. So, wouldn't it be wonderful to have the money to build a whole new public service IT system? But that's just not reasonable. That that would occur in some utopia, unless the Department of Finance is looking at that?

NARELLE DEVINE: We'll ask the question to that questioner.

ABIGAIL BRADSHAW: What a shame. So, along with that – along with that recognition that there are different systems and their very, very different IT requirements – I think you have to accept that we wouldn't want to ever suggest that we – from a central perspective – know the needs or want to manage the risks of each one of those agencies. Because agencies themselves will understand those needs and how they want to manage those risks themselves. So I think the best way to approach this from an enterprise perspective is actually start with some key principles, rather than a strict compliance framework.

And we try to do that through the PSPF, which AGD own. And in the ASD sense, we have responsibility for the Information Security Manual for the Essential Eight and mitigation strategies, which we publish in a principled way, in a way which is informed, for example, by items like the maturity model, which enable the maintenance of that autonomy to manage risk, resources and needs on a unilateral basis, but by achieving a principles approach.

HAMISH HANSFORD: Can I answer that from a really practical perspective, to demonstrate to Finance how innovative we've been within existing budget allocations over that period?

HEATHER COOK: Shamelessly!

HAMISH HANSFORD: And even the change that's happened over the last six months by using Skype, by using WebEx and Microsoft Teams, I don't think I've ever seen the amount of video conferencing and collaboration at a video to video level across the Commonwealth. So I think we've demonstrated that if an experience like COVID-19 really impacts us, we try and respond pretty quickly. And in a department that has 14,500 people, with the majority of people able to work from home or have the capability to work from home, particularly at the height of the COVID experience, then I think we really demonstrated that we can agilely and flexibly move to that model more strategically though.

I know Randall's with us from the DTA today. I mentioned in my initial remarks that the Secretaries Digital Committee is looking at the policy issue about how do we become a much more digital government? How do we deliver services in a much more digital way? The flip side of that is, well, how do we do it in a more secure way as well? And I'm aware of the fact that we were looking at the issue of, how do you centralise cyber security arrangements to get the best effect out of the existing mechanisms we have in place? And how do you aggregate some of those to respond in a much more consistent and dedicated way to try and actually build expertise on a continuous basis? So, I think that's the two answers I'd give to our finance colleague.

HEATHER COOK: Thanks so much for that. Let's open the floor to some questions. I think we have IPAA staff who have microphones. They'll be sanitised in-between use. But raise your hand if you've got a question and we'll handle a microphone across.

BOBBY CERINI: Thanks. Bobby Cerini from Questacon. Abigail, you mentioned the sense of trust in the Australian people. My question for the panel is, who do the Australian people trust when it comes to cyber security?

ABIGAIL BRADSHAW: How about I give that a crack. Well, I think they trust us to be honest. And I think I can safely say that it's not me blowing my own horn. But actually, those results that I told you about earlier, that copy and paste advisory that was downloaded so many times, the fact that our call centre has taken a 200% increase over Q3 last year to Q3 this year. I think it's a KPI that we can rely on safely to suggest that Australians trust the ACSC.

I think the important issue for us and the difficult area is how... because cyber is part of all about business, how do we unify our voice to ensure that we don't proliferate or make it more difficult for Australians to access an authoritative voice? That's why we work so closely with the Safety Commissioner and the ACCC and the ACIC... oh so the Australian Information Commissioner, to ensure that we really stay in our lanes.

So my lane, I'm in no way confused about my lane. It's about technical cyber security advice. And to the extent possible, we engage with each one of those agencies as we release products, as we produced comms strategies and regimes, so that we are able to not only ask for their amplification of our messages and the referral of inquiries to cyber.gov.au, which is an excellent website by the way, but also, so that we're able to amplify and redirect inquiries that appropriately belong elsewhere. It's not to say... I mean, it's a great question because there is work to be done. We've done quite a bit of market research this year to assist us, as we go forward in our next 12 months of campaign, around how to ensure that people know and Australians know where to go to get advice that's relevant to them and to their particular concern.

So, if you click on cyber.gov.au, and that's a blatant pitch. You should. That website is actually – Well, we host it and the ACSC, but it's actually not about us – it's about our target audience. Unlike a lot of Public Service or even corporate websites, when you click on cyber.gov.au, it's not about the ACSC. It doesn't start with, "This is our leadership; this is our mission, et cetera." It actually starts with our audience.

So, people are able to actually click on I'm a business or I'm a family or I'm a government service and obtain the advice that's relevant to them. I think our focus for the next 12 months will be to continue to leverage from that through a variety of different means through social media and through a rolling campaign on cyber security. So, for us, we say there's no such thing as cyber security day, or cyber security week, or cyber security month. Every day is cyber security for us. I think to go to your question, how we increase that confidence is making our advice more practical, and usable, and consistent with the needs of each audience, and ensuring that we maintain that constant drum beat of engagement.

BOBBY CERINI: Thanks for that.

JUSTINE GOUGH: Yeah. I think it's a challenging question. It's a difficult question. It's a very, very broad question and I would certainly concur that... And you've heard it from a number of panellists, one united voice, consistent messaging, et cetera. I think that probably there's a number of players that can contribute to the messages that joined to the awareness of the community.

Also, included in that is, of course, state and territory police who do have interaction with the community each and every day and do play a part in terms of investigating reports cyber and supporting the victims of cybercrime across the country. So certainly that's a challenge and a role for the AFP to coordinate with state and territory police and to provide the lessons and, I suppose, the learnings that take place in relation to the criminal threats across the country to incorporate those into the prevention messaging that is coordinated centrally, so there is one united message.

HEATHER COOK: Let's grab another question.

PATRICIUS HEUSSER: Hi, everyone. I'm Pat from Department of Infrastructure. I've just got a question, it's on the physical cyber-nexus. So we're looking at critical infrastructure as well, obviously, and more so than just critical infrastructure, also emerging technology as well and the security of emerging tech. My question is we're seeing a lot of traditionally civil engineering projects transition more and more into being cyber projects. And so I would ask, how do we underscore the resilience of future systems maybe that we don't even know will be almost predominantly cyber systems?

HAMISH HANSFORD: Well, thanks. A really good question. I think that's a really big challenge for government and for industry. The government started a discussion with industry about, how do we collectively improve our supply chains? And so, the governments put out supply chain principles for consultation. Some of the key aspects of that consultation is around Secure by Design and transparency, and how do you try and make a future prosperity agenda for the government in line with the Prime Minister's statements about the digital agenda out to 2030? But how do you do that in a secure way?

So, I think the government has really started the discussion and the collaboration with industry on the supply chain side, and that really does flow down to whole of economy. The government has also put out an Internet of Things Code of Practice, which gives some pretty strong signals for what products you should buy and what products you should buy as a service. For those companies, particularly those involved in product development and supply and service development, they're really good guidelines about what the future secure Internet of Things will be about. So I think it's both an emerging challenge, but one the government started to consult with industry and to put out some initial guidance.

NARELLE DEVINE: I think on our side from an industry, we probably have the same challenge. We're building things and we're rolling our infrastructure. They're probably things don't exist now: the threats don't exist to those things. The way we're approaching that is a really strong awareness campaign and a education campaign throughout the entire company, so it's not about cyber being done just by my team. Cyber needs to be done by everybody.

Because as they are developing these new products or looking at what we do next, if they understand the threat and they understand the trends, they're far more likely to have a look at, as you said by Secure by Design, they're far more likely to look at what they're about to do and go, "How might this be used against me or how might someone maliciously try and use this?" And so by doing that, our hope is that we're able to then build in security we may not even be aware of, to be honest, and not be teaching to last year's texts, if that makes sense.

HEATHER COOK: Other questions?

AUDIENCE MEMBER 3: It's really great to hear the strong industry collaboration and also the state and territory police interactions. I'm really keen to understand a little bit more about the state and territories, and how you work with them. So most of our... or not most, but a lot of our really big risks exist in our hospitals, in our transport, in our schools, in our smart cities, which are being developed by state and territories. I'm just keen to understand a bit more about that?

ABIGAIL BRADSHAW: Sure. How about I start? So, we in the ACSC have a thing called the National Cyber Security Committee. That's right. I co-chair it with, at the moment, the Victorian Chief Information Officer, a guy called John. They're all called John or Tony, I find, but we meet regularly. This year we have met more than 30 times. That gives you an indication of just how connected we are. So, and that's at a sort of SISO CIO level. That group has a series of subgroups, which work on operational matters constantly. And in the same sort of regular exchange, which I described that we enjoy globally, we meet at both an unclassified level and a classified level.

There is a set of... a framework, for example, for cyber incident management. We collectively determine, on at least a fortnightly basis, what we regard the national incident management level to be. And we debate that robustly. We share what we are doing, for example, a huge amount of interest this year. Hamish has joined at least 10 times, I think, that forum to share the Commonwealth view on the strategy and the programs, a huge amount of interest from the States on CESAR. And what we're doing operationally and how they can absorb the benefits and then what speed and at what pace and how they can match those programs with, at the state level, with local programs that don't try and overlap, but actually complement those central capabilities.

We talk about not only operational matters, but matters like, for example, workforce. The need for us to grow a huge number of cyber specialists in the future. And the fact that we'll all be competing for the same workforce. We talk about state collaboration centres. So, I mentioned the Joint Cyber Security Centres. There are excellent examples of where similar collaboration centres are being generated on a state basis because of their acknowledgement of the need for collaboration, and to have central places for people to come together, to do the sort of teamwork that you need in cyber.

And a classic example is in Adelaide ‘Lot Fourteen’. I mean the South Australian Premier is one of the best advocates in cyber you could get. He's at ‘Lot Fourteen’ every five minutes announcing something new, or supporting some new program of work. And we engage through our JCSC and, whenever we can, remotely with that work as well. It's incredibly important, particularly valuable also, by way of example, in sharing our information about state-based actors and that level of attack, which has happened this year. That forum enables a sense of collaboration and shared risk where, just as we do on a global level, those State CIOs are awesome at sitting forward and saying, "Listen, this has happened to me this week. This is terrible. This is how I'm coping with it." And openly sharing with state colleagues so that they can learn from the impacts of what other state colleagues have seen.

HEATHER COOK: And from a law enforcement and justice perspective, there's, I think, increased emphasis on cybercrime and the threat it poses to the citizens of states and territories. And there are a lot of collaborative arrangements that are in place.

There's a joint management approach to cybercrime as one of the state and territory and Commonwealth areas of focus and there's collaboration in relation to specific themes of cybercriminal activity. So, for instance, business email compromise, remote access trojans, and obviously actors from a different location, people impacted in various states around the country. So, a need for collaborators and certainly a need for coordination in relation to those activities. We can always do more. And certainly that's a focus, I think, across all of the state and territory policing agencies that cyber is such an important element and we do need to increase our capability and capacity across the board. So there's a good kind of starting point and we can only enhance from here.

HAMISH HANSFORD: You understand Heather, that we have a four-way discussion with states. One of the ways is through the SISOs that Abi's mentioned in the NCSC. We also have a good conduit through first ministers and prime minister and cabinet, including through the national coordination mechanism. And we've had lots of discussions on critical infrastructure protection and policy discussions with police agencies, including the government's commitment to a joint capability fund with state and territory police. So, that's another way. And then more generally with... Through regulators as well, and obviously critical infrastructure resides in states and territories. And that's the kind of fourth way. So lots and lots of discussion with states and they're critical to any policy reform, any operational issue.

HEATHER COOK: Very much. Questions next.

DIRK NOODEWIER: Hello, Dirk Noordewier. We've spoken a lot about security today and we also made the comment, someone in the panel might comment about safety and the take-up of the public awareness towards cyber security. I guess my question is from a safety and security perspective in the physical world, that's fairly obvious to everyone. The part that I struggle with, and I suspect that many others would, when we get into the cyber world, the lines get a bit blurred between security and safety. So, I'd just be really interested in the panel's views on those two aspects, or are they indeed one aspect, in the cyber space.

HAMISH HANSFORD: I'll kick off and we work, I know the eSafety Commissioner representative, Janelle's here today, but I think it's a big kind of continuum. And at one end security, one and safety, and we kind of approach them from two distinct areas in terms of regulation and operational response. And there's criminality as well, tied up in there. And, you're right, often they do intertwine. And when you're trying to teach a child to be safe online, it's also good to teach them to be secure online. So, not only worry about who you're talking to, making sure that you have locked down closed networks, but also changing your password, making sure that that's kept up to date. So, they are complementary, but in a sense they are two distinct issues that do intertwine. And I think that the criminality aspect also kind of intertwines as well.

NARELLE DEVINE: Yeah, I would certainly echo Hamish's comments in relation to that. I think that the point that I would probably raise is that I certainly observed from my agency's perspective, that the level of cyber literacy needs to increase to combat the challenges that are posed. And I would probably say across the entire community, the degree of cyber literacy needs to elevate because there are elements of security. There are elements of safety. And I think that that's certainly very key to the prevention awareness messaging that we do need to focus upon into the future.

HEATHER COOK: Probably have time for one more question from the audience. Oh, Caroline?

CAROLINE MILLAR: Thank you all for such a wonderful discussion; I've learnt a lot this morning. I've heard a lot about the relationships and it's wonderful to know that everyone seems to be in lockstep at the federal and state level. And I know that those are the two levels of government that are constitutionally enshrined, but there is also the local government level. And that sort of comes in when sort of talking about smart cities and also collaboration and looking to industry. It would be wonderful to hear some remarks about that level of government and how they tie into the strategic framework.

HAMISH HANSFORD: Sure, why don't I kick off. And the government was really conscious of how do you impact an individual victim on the ground and how do you try and make sure that the messaging at the strategic level through cyber.gov.au is really flowed down into all of the economy.

So maybe I'll just pick up on two measures, one of which is victim support. So, there's a key NGO who focuses on assisting individual victims through IDCARE based out of Queensland. So, they're on a day-to-day basis dealing with individual Australians, in addition to the police and our state and territory and Commonwealth, but really kind of good example of the government, both tackling the strategic issues and effectively existential threats to the society and economy and security, and then looking at individual victims as well and putting funding into individual victim support. So, that's kind of one measure.

Another one, which is in the strategy really goes to chambers of commerce and peak bodies. And how do you try and get information down at the community level, through networks of industry and networks of individuals at kind of a more community level. And so, there's funding in the strategy through the Department of Industry on a grant basis, to try and make sure that those bodies are also involved in messaging cyber security responses, prevention, and a whole range of initiatives tied back to cyber.gov.au. And kind of the final point is Abi mentioned the Joint Cyber Security Centres, which were obviously set up in the 2016 strategy. And the government's invested money to build on those as well, and be real focal points of the state and territory community level as well, and dedicated funding for outreach officers to work with ACSC, to try and put out messages, bring together people to share information and try and do that at a community level.

ABIGAIL BRADSHAW: Yeah, I might just echo that comment and it's interesting because I ... My most recent job was the national bushfire recovery at the beginning of this year. I always wonder about that on a CV because I'm sure people go, "Bushfire, cyber? What's going on there?" But I learnt so much from that experience about Australians and the way they respond to information and services, and how they access them and what's really important. And what I will always take away from that experience is the importance and the profound influence of local councils and Local Government Areas (LGAs). I mean, outside of Canberra land, it really is how real Australians operate and they're fundamentally important.

And that's why our Joint Cyber Security Centres are important, because actually cyber security doesn't happen in Canberra for the 400,000 odd, relatively privileged people here. It happens for the real people that actually live in LGAs. And so, the Joint Cyber Security Centres are really an extension of the ACSCs that give us a presence where cyber security really matters and where it happens. And if you have a look – and I do every week – at what the joint cyber security Centres are doing, they are doing something different everywhere.

And it's obviously a national program, but the education and collaboration and talks, information sessions that they are coordinating and running are directed at local issues and local concerns and local needs. And the opportunity here for us is, as Hamish said, to take that investment in the Joint Cyber Security Centres, which will enable us to send classified information and to sponsor security clearances for appropriate people in each one of those states and territories, to be able to consume that information and find a way of moving it where it needs to go in an appropriate format. But to work more closely with the LGAs, with the local councils, to ensure that the information that's getting to customers, communities, and small businesses that are lifeline of Australia, actually suits their customer needs.

HEATHER COOK: Thank you very much. I think we are out of time. So, that was a very, from my perspective, very exciting and interesting panel discussion, not only looking at the challenges, but some really encouraging evidence of genuine initiatives and progress in this area around awareness raising and building resilience. And my strong takeaway in listening to the panel that we've had here today is certainly that it embodies that team approach to it. That it is a team sport, and I certainly saw a great deal of evidence of that today. Can I also thank the participants both online and here in the room for your interest and your probing questions, which added a richness to the discussion as well, much appreciated.

I'm going to offer the panel each a 60 minute or less opportunity to share some final thoughts or takeaway for the group today. I know some were speaking a little bit slowly so that they can start formulating their thoughts around that. But speak from whatever lens you would like, but perhaps consider what 12 months from now should look like in terms of progress, from your perspective. Let's start off with Narelle, down the end.

NARELLE DEVINE: So I think in 12-months time, as I said before, it is about having even greater threat sharing ability, ability to speak to each other, ability to share in general. And that's just not across industry and government that goes all the way down to the mums and dads out there. How do we get that message out there and being able to articulate a message that is understood.

And as we've said repeatedly in the last hour or so - that is very consistent, and that we're able to help wherever we can to do that in whatever area we sit in, but we're all working from the same song sheet. And I think it really is a team sport. There is not a day goes by where I don't talk to, not one or two SISOs out there, but I would say 10 to 15. We talk all the time. So, for any of you that think that maybe we're not joined up and we're not engaging, it couldn't be further from the truth in the background, we are sharing all the time. And it's now just about how do we do that in a more automated, quick, quicker fashion, and how do we bring more people into that trusted circle.

HEATHER COOK: Thanks, Narelle. Justine?

JUSTINE GOUGH: I think very well said, Narelle. Look, I think that I will probably just reflect from a purely a law enforcement perspective. I'm very encouraged. And I think that the partnership approach that we have is excellent and really the key for success in the future. The challenge in terms of AFP, and I think state and territory policing, so that we can actually be effective in the arrest and prevention, sorry, arrest in disruption space, is increasing our cyber capabilities and our capacity across the country. It's about cyber uplift, not just about our specialist cyber investigators, but our general cohort of investigators as well. And I think we have some significant challenges in terms of recruiting for that type of situation into the future. So, we're certainly very interested in any talented individuals that you might know who may be interested in joining the AFP. And we're certainly looking forward to recruiting for that type of future.

HEATHER COOK: Thank you, thanks Justine. Hamish?

HAMISH HANSFORD: Well, the threat environment in terms of the cyber landscape is changing so quickly. So in 12 months time, who knows what to expect. But in 12 months time we'll have a well-grounded new regime that is based on the rule of law, that is well articulated through policy, that has good playbooks in place, that is exercised and will be a fit to deal with any challenge in the cyber regime or cyber world that we face into the future.

HEATHER COOK: Thanks so much for that Hamish. And we'll leave the last word to our keynote speaker today.

ABIGAIL BRADSHAW: Okay. So I'm going to try and limit it to 60 seconds rather than 60 minutes.

HEATHER COOK: Oh, did I say 60 minutes? Oh my God.

ABIGAIL BRADSHAW: Just feel like we're getting warmed up. So, I feel incredibly optimistic about the future, to be honest, and especially so having my besties here. I feel really optimistic about team Australia. I feel like it's almost a public servant's dream actually to walk into a job with an industry advisory panel headed by leaders of industry with a comprehensive sensible series of recommendations that is then responded to by a Cyber Security Strategy, which makes in my view pretty logical areas of prioritization, in which you're able to focus on critical infrastructure, cybercriminals, small to medium enterprise, protecting the victim in that sort of logical, sequential sense.

Then to have the legislative frameworks roll out so that we have a legislative framework, that again, is consulted heavily with industry to provide a framework for a more robust system of protections for critical infrastructure and systems of national significance. And, of course, in the law enforcement space, a legislative framework for so-called dark web powers. And then, of course, to underpin that in the case of the ACSC, I feel incredibly privileged to have that funding to feed, to optimise and to deliver on those critical components of operational capability that appropriately sort of meet the objectives of the strategy, the legal framework and the needs of the Australian community.

So, I hope to be sitting here again – if that was an invitation Heather? – in 12 months, to be able to look you all in the eye and all those things that I set out in my opening speech, where I said, this is what we're going to roll out. I'd hope to be able to give you a really optimistic and useful, fruitful readout on what we have delivered.

And the best bit about 2020 – and there's so many bad bits you can take away from 2020. My lowest point was an algebra lesson with my 14 year old on Zoom. It's an experience I never want to go through again – but one of the great bits about 2020 actually – and I've had the benefit of seeing this both through the National Bushfire Recovery Agency and through cyber – is we have the incredible Australian spirit, that the response of Australians to the Prime Minister and the Minister's statement on the 19th of June was absolutely incredible. You've got people that are alert, aware, calm, engaging, and we know they are absorbing our messages.

And so, other than having a strategy mandate money and a willing customer set, there's – and fabulous partners, as well as industry partners – there's not much more that a cyber gal could wish for, Heather.

HEATHER COOK: Terrific. Thank you so much for that. Thanks again to our excellent panel today for sharing their thoughts. IPAA would like to take the opportunity to present you with a small token of appreciation; some award winning chocolates from local chocolate maker, Jasper and Myrtle. But can everybody please join me in thanking our panel today and our keynote speaker?

So before we kick off a bit of networking, which I'm sure we're all looking forward to, can I do a couple of shameless plugs for some upcoming IPAA events before the end of the calendar year. On 25th November here at the National Portrait Gallery and as part of our *Secretary Series*, we have Secretary Mike Pezzullo who will be here speaking from 9:00 to 10:00 AM. And later in December, on the 8th of December, we have *Public Policy Lessons from the Global Financial Crisis*, also here at the National Portrait Gallery in the morning, 09:00 to 10:30 AM. Go to the IPAA website if you're interested in attending. You can register there either for online participation or to be physically present in the room. But obviously those tickets to be in the room are quite limited so move quickly if you're interested in either of those events before the end of the year.

Can I also take the opportunity to thank IPAA's partners, KPMG, Hays, Telstra, MinterEllison, Commonwealth Bank of Australia and Microsoft for their ongoing support for the IPAA's program. And can I invite those that are in the room to join us for a bit of a networking opportunity? I know we get few and... Those are few and far between for us so please join us. We are, as I mentioned before, doing it in a COVID safe way. So, refreshments will be served at the table in individual portions, but you're free to get up and walk around and have a chat to everybody. Just keep in mind the social distancing rules, if you would.

Thank you again for your participation. And can we give another warm welcome or a warm appreciation to our panel?