PwC Public Submission

Australia's 2020 Cyber Security Strategy

November 2019

www.pwc.com.au

pwc

Executive summary

The Government's role in Cyber Security

The Government's role in cyber security is to reduce the harm caused to Australia, its people, and its businesses from cyber attacks and incidents. Whilst great strides have been made since the 2016 Cyber Security Strategy, the Australian Government can help make Australia an even harder target for cyber criminals, and build a more resilient cyber security culture that increases safety for all Australians.

To play a leadership role in enhancing Australia's cyber security, the Government must operate from a position of trust. Securing Government systems and delivering secure digital services will enhance trust in the Government and their ability to take a leadership position, especially should it take an active role in the cyber security of the private sector. Another method of enhancing trust is to lead on privacy and security-enhancing protections for citizens, such as new legislation to limit how the public and private sectors can collect and use the biometric data of Australians.

Reports on cyber resilience in the Federal Government by the Australian National Audit Office (ANAO) show substantial work is required in many Government Departments and Agencies to achieve the mandatory ASD Top Four mitigation strategies. The Government's low cyber security maturity presents a challenge for it to assert a leadership position. Strengthening cyber security resilience in Government agencies and programs will build capacity, skills and trust in Government as it continues a shift to digital service delivery. Introducing programs such as a funded public bug bounty will improve security and underscore a forward-looking commitment to innovation.

Australia's critical infrastructure enables the services that everyday Australians rely on to live and work. Given the potential for harm should these services be disrupted, protecting critical infrastructure must be a Government priority. In deepening the Government's role in critical infrastructure protection, care must be given to work closely with industry - operational technology networks can be complex and fragile, and the knowledge of how to operate and secure them safely is limited.

The Government has an opportunity to play a coordinating role with the private sector and lead the sharing of cyber threat intelligence. The JCSC program was a great first step but has not yet reached its potential, and could be an engine room for high-quality threat research, and a more community-driven hub of activity. JCSCs should be injected with additional analyst capability to develop sector specific threat intelligence products that can be distributed to partners.

The importance of protecting customer data for both Government and industry is critical to Australia becoming a data-driven digital and prosperous nation. Government can set the conditions to improve cyber security across the supply chain by supporting small and medium businesses to improve their cyber capacity. Supply chain risk management is a disconnected activity, where more mature businesses interrogate organisations in their supply chains, but smaller businesses in the supply chain often lack the resources to engage with supply chain assurance processes conducted by their customers, which can all focus on different concerns. Australia can make advances by reducing duplicated effort in supply chain assurance and by assisting small and medium businesses to build cyber resilience. Working closely with industry, Government should lead development of an agreed set of standards for supply chain security to streamline and simplify the assurance process for governments and industry.

We believe Australia should continue to build cyber security skills in its people. The Government should consider introducing more TAFE and higher apprenticeship pathways to give more Australians the opportunity to forge well-paid careers in an area of skills shortage.

Prime Minister Scott Morrison has described Australia's democratic process as 'our greatest asset, our most critical piece of national infrastructure.'1 Australia's democratic infrastructure runs beyond electoral commissions and includes political

1 https://www.pm.gov.au/media/statement-house-representatives-cyber-security

parties, think tanks, and associations. The Government should act to enhance protections for Australia's broader democratic infrastructure and safeguard our democratic process.

Lastly, Government should have a long term focus on 'What's next?'. While individuals come and go, and companies rise and fall, long-term stable governments are particularly well suited to consider the effects of trends like the emergence of artificial intelligence and quantum computing on our long-term cyber security. These should not be party-political issues, but ones addressed for the long term prosperity of our nation. What can Government do to shape the future development of these technologies to minimise harm while harnessing the benefits they might provide?

The remainder of this submission paper covers the themes above in further detail.

Contents

1. Securing Government

In order to achieve its goal of a safer and more resilient Australia - with less harm caused by cyber attacks and incidents - the Government must lead by example and represent a beacon of good practice. Trust from business and the general public will only be strengthened if the government is seen to be taking cyber security seriously for its own entities across the whole government space, not only at the Federal level, but also State and Territory[2]. This means visible high levels of investment, demonstrated improvement in maturity, and strong & prominent leadership by senior people.

A unified 'whole of Government' approach should be reflected in the Strategy to demonstrate that Federal, State and Territory Governments are aligned and working together to improve their own cyber security.

At present most of the public conversation from Government is about the 'hard and pointy' end of cyber security - offensive cyber (ASD, ADF); law enforcement tackling cyber crime; periodic statements by the ACSC on the high level of threats to Australia, and news about increased investigatory and intelligence powers for agencies to try and disrupt potential criminal/terrorist activities. We believe there is an opportunity for the Government to talk more transparently about how it is improving its own cyber security hygiene, which in turn may encourage more organisations to adopt similar approaches in communicating outwards to their own customers and consumers.

Given the media attention to the importance of election security, this would be a great topic to be highlighted in the Strategy as a case study to show how hard the Government is working to secure this (the fact that the ASD is working with the AEC is a real positive).

Drawn from our experience of working with a wide variety of organisations and delivering cyber security services in many countries around the world - Australia, Asia, Middle East, the USA and across Europe - there is a demonstrable difference in attitude and approach from the public and organisations when the Government is able to point to itself as an example of good practice for cyber security. It also helps when there is clear articulation of roles, responsibilities and accountabilities for all the different aspects of government, simple machinery of Government for cyber security and privacy, and evidence of partnership working between Government and the private sector.

Below are some further suggestions for how the Government can articulate and evidence how it is improving its own cyber security:

- Establishing a cyber security maturity target to be reached by all government entities by an agreed year, and for annual reporting on current maturity levels. Ideally this would allow Government standards and frameworks such as the ASD Essential 8 and the PSPF to easily map / align to more broadly adopted frameworks such as the NIST CSF. This will help drive further uptake across all levels of Government, and encourage cross-sector benchmarking and comparison across industry.

- The ACSC could also conduct random ACSC red teaming programs (e.g. red team assessments with the ANAO) across the Commonwealth. Each assessment results in a report provided to all Secretaries, and should feed into the maturity reports made by each entity.

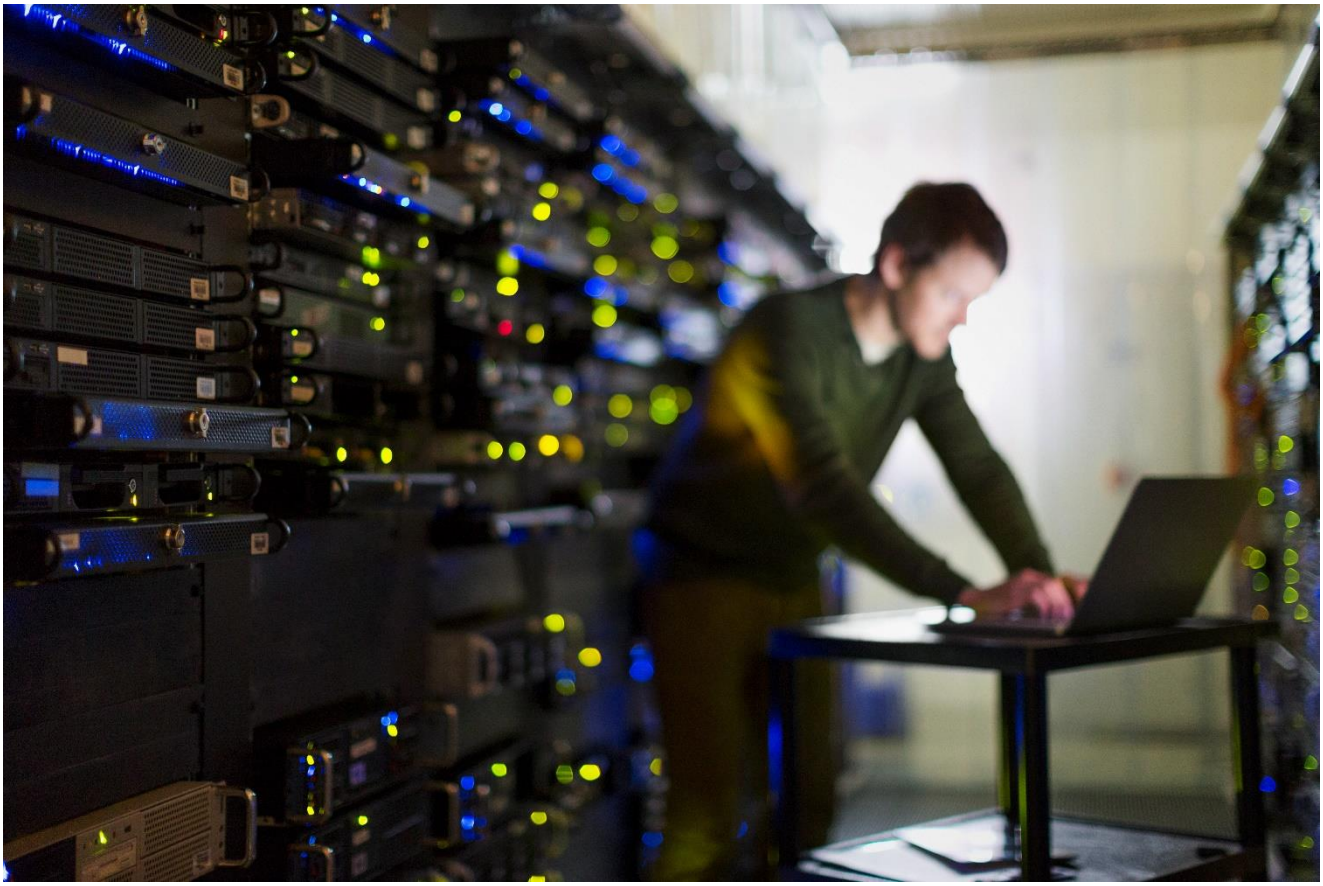
- Stronger awareness campaigns about what Government is doing to improve cyber security and why it is a priority, linked to protection of the public and their data, critical services/infrastructure, and the need to lead by example. If the Government adopts an Active Cyber Defence program similar to the UK - which would be a very positive step - then the awareness campaign can also cover how this is making Government entities themselves less vulnerable, as well as businesses and individuals across the country.

[2] The digital My Health Record, where 2.5 million Australians to date have opted out, is an example that points to the relatively low level of trust in Government to protect sensitive citizen information. In addition, a number of public audit reports have highlighted areas requiring significant improvement, including the ANAO, NSW Auditor General in 2018 ('Detecting and Responding to Cyber Incidents') and Victorian Auditor General's Office in 2019 ('Security of Patients' Hospital Data')

- Introduce bug bounties for Government entities, a concept that has proved successful in several countries including the USA where the Department of Defense launched a 'Hack the Pentagon' program in 2016, representing the US Government's first Bug Bounty Initiative. This program uses highly vetted ethical hackers to find vulnerabilities in DoD websites and assets. The program was extended to award contracts to vetted private sector firms to create partnerships to find bugs in sensitive internal DoD assets as well. Over 8000 valid vulnerabilities have been exposed since the program started. The DoD is now working with private sector partners to bring crowdsourced security activities like this to other departments. Singapore and Switzerland have also introduced similar concepts. These programs have the benefit of encouraging organisations to hire more internal cyber security staff in order to remediate the bugs found - it can become a virtuous cycle for improving cyber security and growing the cyber industry.

- Consider centrally provided Enterprise Security Services across government (e.g. DNS filtering, Web App vulnerability scanning), which could at some stage be available beyond Government entities.

- Introduce a 'Secure by Design' initiative and code of practice, and help promote this across industries - and do this jointly with State and Territory Governments.



2. Organising Government to defend against cyber threats

The role of the Australian Government in cyber security will continue to grow as the demand and dependency on the Internet and Internet-connected Devices continues to increase. With increasing threats and fewer opportunities to fail, the Australian Government must rise to the challenge to protect both national security and economic prosperity, and reduce the harm caused to all Australians from cyber incidents.

As a priority, PwC recommends that a Prime Ministerial statement be issued on the way ahead for cyber security - this could be made with the launch of the new Strategy in 2020. We recommend the statement could include:

- A reminder of the challenges Australia faces in terms of cyber security and the benefits to everyone if we step up to this challenge;
- The appointment of a dedicated Minister for cyber security (PwC understands if the current cabinet numbers precludes an additional cabinet minister appointment, it is recommended that a minister assisting the Prime Minister on cyber security be appointed, because of the importance of optimising cross cabinet and ministry coordination);
- The Government host annual cyber security leaders' meetings, where the Prime Minister and business leaders set the strategic cyber security agenda and address significant challenges beginning with supply chain security;
- The Government, through the Minister for Cyber Security, provide annual reports to Parliament on Australia's progress to improve its cyber resilience;
- A Council of Australian Governments (COAG) working group be established to improve the level of cyber security collaboration between the three tiers of government , including ambitious targets and bi-annual benchmarking of progress reported to COAG. This demands that an aligned method/framework of demonstrating maturity improvements be adopted;
- The ANAO be tasked to review cyber security collaboration across the jurisdictions annually; and
- The Australian Local Government Association (ALGA) be enabled and resourced to undertake practical initiatives to uplift cyber security resilience across Australia's 537 local councils - a majority of which are responsible for essential services for all Australians, and currently lagging well behind regarding cyber security.

PwC recognises recent efforts by the Department of Home Affairs and the ACSC to improve collaboration across Government but we believe more needs to be done as we address increasing threats to essential services across Australia, in particular, addressing increasing supply chain vulnerabilities within our critical infrastructure, defence, industry and research sectors.

When we consider the costs of recent cyber security compromises here and overseas (Ransomware NotPetya was estimated by the White House to have caused $10 billion USD in damages globally[3]) PwC believes more investment is needed to strengthen Australia's cyber security resilience.

The Government should undertake significant investment in the Australian Cyber Security Centre (ACSC). This investment needs to be targeted, measured and allocated in a decentralised model that grows cyber security capability in capital cities through the JCSCs, and enables the ACSC to draw on wider resources pools.

The ACSC should be led by a Secretary-equivalent to better reflect the current expectations on the organisation to support all Australian Government, industry and everyday Australians. Additional investment will enable the ACSC to deploy its analysts in various industry sectors to better understand and address current and emerging vulnerabilities, working closely

3 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

with cyber security industry counterparts. This is a key ingredient that will help to enable many of the suggested initiatives in our submission.

PwC recognises significant private sector investment is also needed for Australia's cyber security resilience. We believe the ACSC needs to take new, bolder and more forward leaning approaches to how it engages with the private sector. We believe the ACSC should engage private sector partners as part of a broader program to encourage individuals and businesses to take the basic steps required to prevent the majority of high-volume, unsophisticated cyber-crime. This has proven to be effective in the United Kingdom through its CyberAware program.

PwC believes the ACSC should enter into time-bound 'strategic partnerships' with specific Australian companies who are able to co-invest into efforts making specific sectors more cyber resilient. For example, we suggest that the Perth JCSC enter into a strategic partnership with an Australian mining company working together on practical initiatives to uplift cyber resilience in the broader mining sector. These partnerships could be reviewed annually providing opportunities for other companies to participate.

PwC recommends the ACSC should commence a program of 'reciprocal cyber resilience engagements' with key providers of essential services across Australia. For example, a private sector organisation providing telecommunications services would invite a team of ACSC analysts onto their network to better understand how that infrastructure works and where vulnerabilities may exist. In parallel, cyber security staff from the telecommunications organisation would be invited to spend time at the ACSC to better understand how current and emerging vulnerabilities could be effectively addressed in their sector specific environment. At the conclusion of the exchange, a joint confidential report summarising the activities (vulnerabilities identified and mitigations implemented) could be provided to both the leadership group of the telecommunications organisation as well as the relevant Minister responsible for that portfolio, the Minister for Communications, Cyber Safety and the Arts.

This program could be scaled over time to include organisations across all Australian providers of essential services.

3. Protecting critical infrastructure

The increasing interconnectivity and digitisation of critical infrastructure assets in our modern digital society has resulted in a number of benefits for organisations, governments and citizens. However it also brings increased risk of disruption via cyber attacks, with a range of threat actors seeking to potentially cause harm to critical infrastructure and services. These attacks can result in significant impacts including health and safety and environmental damage, and demand different approaches in detection and response capabilities, compared with more data-centric attacks and breaches. The 2016 Strategy focused more on privacy and confidentiality risks - the opportunity for the 2020 Strategy is to equally focus on availability risks that can impact our national interest and our communities.

Currently, many critical infrastructure operators in Australia do not have the capability to adequately protect their environments from advanced threat actors. From our recent experience working across critical infrastructure sectors, most organisations are still building foundational cyber security capability. As an added challenge, these organisations are now competing for the same talent and resources with more advanced sectors (such as Financial Services) who have well-established capabilities and career paths for cyber security professionals. There is a real risk that without significant government support, our critical infrastructure sectors will continue to face these challenges in uplifting cyber capability, resulting in an increased likelihood of disruption to Australia's critical infrastructure and services via cyber attacks.

To better protect our nation's critical infrastructure, the Government requires much closer partnerships with the relevant critical infrastructure owners/operators. This may entail the Government establishing agreements with operators, or via industry regulating bodies, that extend its reach into the private networks where these critical assets sit, for the purposes of detection and/or response capabilities. This interaction with private networks can take various shapes and forms - our suggestion is it should be a risk-based approach to provide cyber security intelligence sharing, detection and response capability for assets not only based on their criticality, but also their current level of cyber maturity. An example of such an initiative is the US Department of Energy's Neighbourhood Keeper program, where they have partnered with Dragos to support the sharing of threat information to critical infrastructure providers, particularly the smaller and medium organisations who often lack their own cyber threat intelligence capability.

PwC believes the objective for the Government should be to support the establishment of cyber 'situational awareness' - in the form of technology, people and processes - across multiple critical infrastructure sectors, in collaboration with industry regulators, specialist vendors and critical infrastructure operators. In this context, 'situational awareness' refers to our ability as a nation, to maintain an up-to-date and holistic view of the cyber security threat and vulnerability landscape across critical infrastructure.

This needs to be done carefully, as many of these technologies - broadly referred to as Operational Technology or OT - are not as resilient or flexible as modern Information Technology networks. The act of integrating with and monitoring these types of networks carries inherent risk, and the ability to establish wide-scale situational awareness across these networks needs to be balanced with the risks of opening up further potential avenues of cyber disruption. It will be critical to look to other countries who have started this journey, a prime example being the National Hybrid Security Operations Centre (H-SOC) for Critical Infrastructure in Israel. Another example can be similarly found in the United States Government agency CISA, short for the Cybersecurity and Infrastructure Security Agency. CISA is responsible for the combined cumulative efforts of the National Cybersecurity and Communications Integration Center (NCCIC). According to the U.S. Government's Cybersecurity Act of 2015, the NCCIC is 'the central hub for cyber threat indicator sharing between government and the private sector'[4].

One of the recent advances in critical infrastructure protection in Australia was the establishment of the Australian Energy Sector Cyber Security Framework (AESCSF) in 2018, which has made a significant sector-wide impact to uplifting cyber security capability and maturity. The work conducted by the Australian Energy Market Operator (AEMO) and the Cyber Security Industry Working Group (CSIWG) is a great example of partnership across industry regulators, Government and critical infrastructure operators. The AESCSF is an important first step to achieving situational awareness for the energy sector, and we encourage the Government to continue to support and expand upon this initiative, and consider how it can be leveraged to apply to other sectors.

4 https://www.cisa.gov/national-cybersecurity-communications-integration-center

One suggested next step is the establishment of a minimum cyber security baseline of key controls that should be adhered to, tailored to various sectors as required, and aligned to a broader framework (such as the AESCSF). This needs to be accompanied by a pragmatic risk management framework to ensure that in cases where the baseline cannot be met (such as technical limitations due to legacy OT systems), there is appropriate guidance or funding (from regulatory bodies) to support the establishment and/or monitoring of mitigating controls and risk-acceptance decisions. Based on PwC's experience, the limitations faced by critical infrastructure operators in meeting minimum cyber security standards are very common across entire sectors, and therefore the Government can make a significant positive impact by adopting this type of approach. The 'reciprocal cyber resilience engagement' suggestion raised earlier in this paper would also compliment this approach.

It is also our view that the current definition of critical infrastructure, as per the Security of Critical Infrastructure (SOCI) Act, requires further refinement for the purposes of a cyber security strategy. Whilst the existing definition addresses key traditional sectors such as water and electricity, it could be broadened to cover other sectors such as transport, manufacturing, telecommunications, agriculture / food production, mining, health and pharmaceuticals, and should consider critical elements of the supply chain to each of these sectors.

With the proliferation of Internet of Things (IoT) devices across many of these industries, and the continued evolution of Smart Cities and their digital infrastructures, we will soon live in a society where every citizen and government interaction relies on a computer-controlled service. The 2020 Cyber Strategy has the opportunity to establish the foundations that will ensure our future cities, communities and the people living within them, can openly embrace these technologies in a safe and secure manner.

4. Protecting democracy

In February 2019, announcing the discovery of intrusions into Australian Parliament House and major political party computer networks, Prime Minister Scott Morrison described Australia's democratic process as 'our greatest asset, our most critical piece of national infrastructure.'

While some of the institutions at the centre of Australia's democratic process are government organisations such as the Australian Electoral Commission, much of our democratic national infrastructure is not operated or directly protected by the Federal Government.

Political parties and their state and territory branches and divisions can operate their own IT systems, and hold sensitive data on citizens, their interactions with politicians and officials, as well as the electoral roll. These systems also contain sensitive political deliberation and strategy, including in relation to elections and campaigns. The intrusion into Australia's political parties discovered earlier this year and intrusions into campaigns and political parties in other allied countries demonstrates the attractiveness of these institutions as a target for foreign intelligence services.

While they attract state-actor cyber adversaries, political parties do not have the capability to effectively counter sophisticated threat actors. Parties operate as lean organisations incentivised to maximise their limited resources on their core business of campaigning. In order to maintain public confidence in the integrity of our democratic processes, the Government must do more to protect our political parties.

While assisting political parties to address cyber threats should be the initial focus of initiatives to protect Australia's democratic process, other organisations involved in our democracy can find themselves facing similar sophisticated threats with limited means.

Think tanks can find themselves in a similar position - minimally resourced with a handful of full time employees and secondees, but privy to non-public statements and meetings with politicians and officials that are of intelligence value to foreign actors[5]. The interaction and communication lobbyists and their industry and community association clients have with politicians and officials as they contribute to the national policy discussion can paint an insider picture for state actors.

We believe the Federal Government has a role to play in protecting Australia's democratic process, including the elements of it that lie outside of the Government's direct control. While we agree Australia's democratic institutions are part of our critical national infrastructure, we think securing these organisations against the asymmetric threats they face requires a different approach to securing our nation's energy grid or water infrastructure.

In particular, our democratic institutions need the freedom to undertake their activities without direct dependency on capability provided by the Government, with particular sensitivity towards anything that could be perceived as monitoring the internal activity of an organisation. One way to achieve this would be to provide grants directly to political parties for the specific purpose of building cyber security resilience and internal capability. With a sufficiently strong internal capability, parties will be able to consume and utilise threat intelligence provided by the Government.

Another method of helping democratic institutions would be to design centralised security services that could be consumed be institutions cost-free. Should the Government develop services like those under the UK Active Cyber Defence program, they should be extended on an opt-in basis to our democratic institutions. Additional consideration should be given to how services may need to be modified to limit the degree to which potentially sensitive metadata is required.

5 Microsoft's Threat Intelligence Center has published research on the targeting of think tanks by state actors:

https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/

https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/

5. Joint Cyber Security Centres

The Joint Cyber Security Centres established under the Government's 2016 Cyber Security Strategy have achieved some of the objectives set for them, but have not realised their full potential. The JCSC program has had highlights - particularly when cyber crises or breaches have affected a large number of JCSC partners. The JCSCs served as a useful coordination point during the proliferation of NotPetya, and after the breach of an Australian business that held data of several JCSC partners. It has also proved a useful 'neutral' meeting place for partner organisations when gathering external stakeholders to tackle cyber security issues on a nationwide scale.

When the 2016 Strategy was developed, cyber security responsibilities had not yet been consolidated into the ACSC and Home Affairs. With pressure to build out the JCSCs quickly, there was little time to test the operating model and fine-tune resourcing. The compressed timeline also contributed to engagement with industry that fell short of the intent expressed in the strategy that cyber threat sharing centres would be "co-designed with the private sector".

While the move for the JCSCs to join the broader ACSC was a positive one, the JCSCs themselves have not been the engine for developing new bespoke advice or intelligence products that they could be. The online threat sharing portal is yet to be developed three and a half years after the Strategy's announcement, and though several interim collaboration channels exist, they are no replacement for a dedicated and fit-for-purpose platform to collaborate and share automated threat intelligence.

The JCSC program is an expensive one, and it is important that the money is spent wisely. It is our strong view that the program should be retained, but it requires substantial change to meet the vision of the 2016 Strategy and to evolve further to counter the cyber threats of 2020 and beyond.

The problem of how to rapidly declassify cyber threat intelligence for use by the private sector is a difficult one. There are real challenges to overcome: speed is critical for the intelligence to have value but going through a declassification process can take time. There are additional barriers where Australia is not the originator of classified cyber threat intelligence and it is received from partner countries at a given classification.

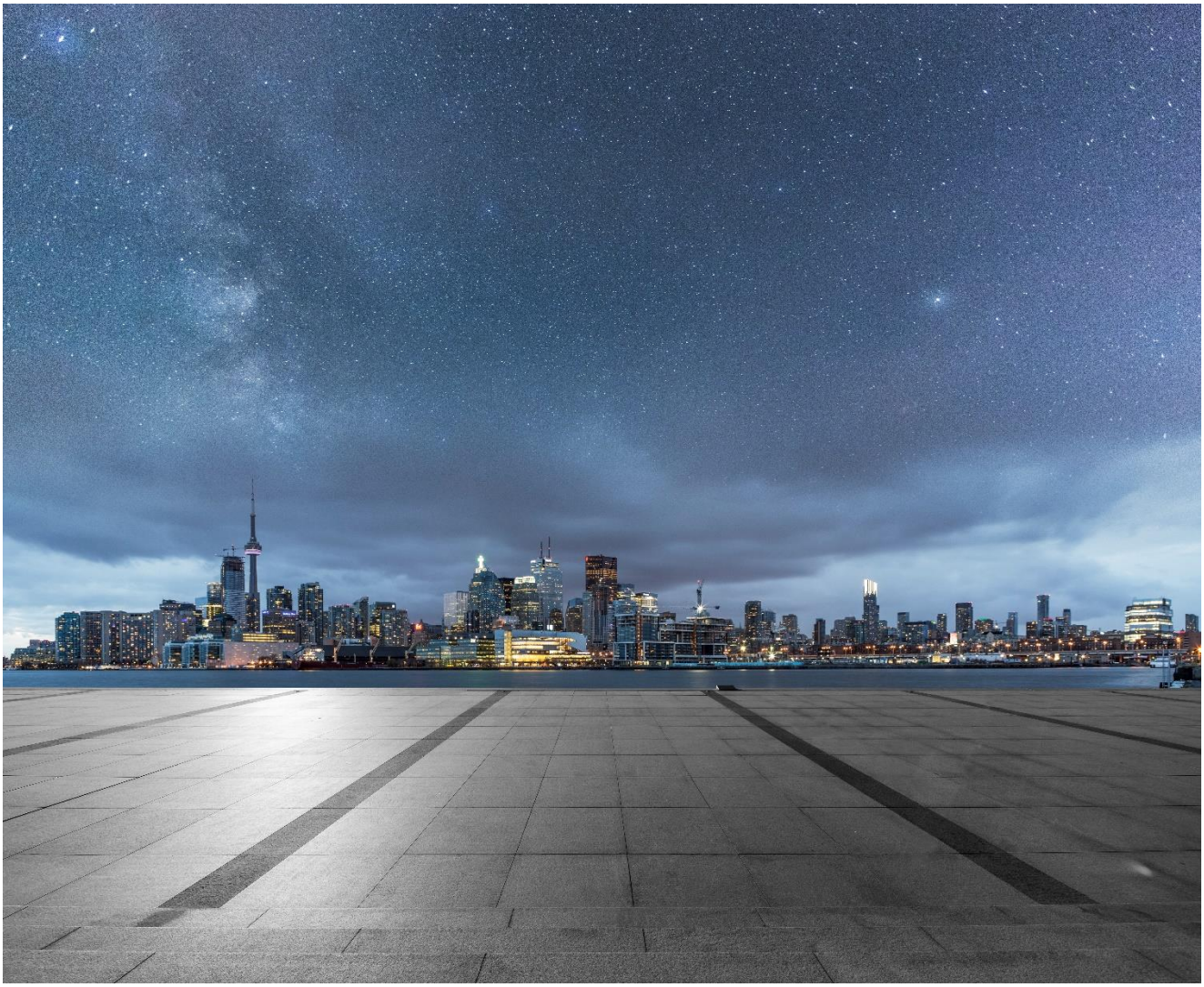
JCSCs have tried some workarounds to this problem, including offering to sponsor security clearances for some private sector JCSC partners. This approach has drawbacks - it is only limited to Australian citizens, and places the cleared individual in the difficult position of having to make decisions on what they can and can't say or do with the information they learn, reducing the extent to which the intelligence is actionable. While challenging, rapid declassification of cyber threat intelligence is an important problem to solve, high-quality near-real time threat intelligence has the potential to increase the likelihood Australian businesses are able to detect advanced threats early.

PwC recommends the ACSC and JCSC review and scale its current capacity to share cyber threat intelligence. Australia should examine the UK NCSC's 'Cyber Security Information Sharing Partnership' approach with a view to better understand what has worked well in its efforts to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.

JCSCs could also be improved by growing a deeper analyst capability, and being a source for high-quality threat research. This could be achieved by the JCSCs employing threat researchers to regularly produce tactical and strategic threat intelligence products. This threat research could draw on open source and classified threat intelligence to produce sector-specific products with an Australian focus. The products should include tactics, techniques and procedures used by threat actors. A good concept already discussed within JCSCs has been building industry-specific centres of excellence in specific capital cities - for instance a focus on the resources industry in the Perth JCSC. In line with a renewed focus on conducting and publishing original threat research in JCSCs, the ACSC should resume publishing an annual threat report.

The Government should also consider how JCSCs can take on a leadership role within their communities. JCSC leaders should be first and foremost community builders, not directors of staff. While greater onsite analyst capability will drive more traffic to JCSCs, leaders should be visiting the offices of their partners, as well as driving membership of JCSCs by evangelising their benefits to a diverse set of audiences. In the spirit of public-private partnership, the Government should consider involving private sector members of JCSC boards in the selection processes for JCSC leaders.

PwC believes a renewed and reprioritised JCSC program would make a strong contribution to making Australia a safer place to live and do business.



6. Skills and workforce

PwC agrees with the statement expressed in the Government's discussion paper that 'access to skilled professionals is an important part of a trusted market'. It is also the case that due to the broad-reaching nature of cyber security in an increasingly digital world, many industries could benefit from improved cyber security related training products. Throughout 2018, PwC's Skills for Australia consulted widely across Australia to understand current and emerging developments in cyber security skills. The purpose was to provide an evidence-based case and industry support for developing common training units to be used across multiple training packages for a range of industries including financial services, business services, mining, automotive and health. Over 150 responses were received, representing 27 industries. Furthermore, all state and territory governments contributed to the consultation process.

The cross-industry, national project aimed to identify, develop and give access to common cyber training skills needs that can be used across a range of industries. It was also specifically designed to supplement a learner's training with cyber related skills alongside their industry-specific qualification, to more effectively and safely complete their qualification and then primary role, as well as become more valuable to an employer with contextualised cyber skills.

PwC consulted nationally and found that stakeholders identified two key issues requiring urgent attention:

- A significant shortage of adequately trained cyber security individuals in the Australian workforce. This aligns with the research undertaken by AustCyber cited in the discussion paper. Furthermore, Australia has seen an increase in cyber attacks, which is likely to exacerbate the problem by increasing the demand for qualified cyber security professionals.

- Lack of industry-aligned cyber security training - there is an opportunity for the information and communications technology sector, and the Vocational Education and Training (VET) sector more broadly to design courses that will help to address the existing cyber security skills shortage.

Through extensive industry consultation, the following cyber security skills needs were identified as a priority:

- A need for basic cyber security skills: employers and training providers indicated a high demand for better cyber security awareness skills among business and ICT users.

- A need for more advanced cyber security skills: stakeholders identified a number of advanced cyber security skills needs:

    - Cyber threat intrusion/detection and response skills, to monitor the network traffic, manage and respond to unusual or suspicious activity on the network to protect a business from cyber attacks.

    - Network and web application vulnerability assessment skills, to identify security vulnerabilities on the network, web applications and produce recommendations to remediate identified security issues across existing infrastructure.

    - Cyber risk assessment skills, to identify cyber risks and ultimately help to reduce Cyber Security incidents in organisations.

    - Managing and monitoring network access control skills, to protect a network from internal or external Cyber Security threats and incidents by applying network security controls such as intrusion prevention systems, firewalls etc.

    - Cyber security incident response skills, to conduct cyber and forensic investigations such as computer memory analyses, network packet capture or malware analysis.

    - Cyber security design skills, to better design digital and computer systems, applications and networks in a secure way, preventing less vulnerabilities by design faults and strong architectural security

- Security strategies for whole organisations, to equip organisations with strategies and organisational best practices in instances of cyber attacks, as well as understanding how to communicate, respond and escalate as necessary

- Secure software development skills, to help guard against security vulnerabilities and data breaches in software or software code.

Other skills recognised as vital for a cyber security professional included effective communication and critical problem solving skills, as well as a suite of traditional and basic level IT and digital skills.

PwC's Skills for Australia has developed a range of training products for the national training system to address these skills and knowledge needs. It is estimated the basic cross-industry cyber training standards will be available early 2020, and a new Certificate IV and Diploma in Cyber Security Specialist training made available mid-2020. We have designed this training in such a way to provide a clear pathway for learners to start, continue or upskill in their learning, dependant on their individual needs and skills gap. The Victorian Government, together with Box Hill TAFE, has also developed an accredited course in cyber security which it has been made available to other public providers for delivery.

The role Government could play in building a market of high quality cyber security professionals:

- Funding for a higher apprenticeship programme in cyber security to encourage employers to take on a cyber security apprentice and build the Australian market. A pilot of the higher apprenticeship programme was conducted in 2017, including in the ICT sector. The pilot experienced higher completion rates (87% for the pilot compared with 61% national average) and better retention rates after the pilot completed, as well as providing employers faster access to trained talent (12-18 months for most jobs).

- Increased subsidies for cyber security training delivery. Subsidies vary between states and territories, between qualifications and between particular population groups which can mean that many people are responsible for the full cost of delivery of a qualification.

- Improved information and resources on cyber security jobs and career support, led by the National Careers Institute.

- Develop a strategy and marketing plan outlining the learning and job opportunities in cyber security, to increase awareness and learner uptake, and link the cyber needs to specific job outcomes

- Create a strategy on training curriculum and pedagogies for greater investment in delivery and material programs across secondary and tertiary institutions.[6]

[6] An example of some work PwC's Skills for Australia has undertaken in this space:

https://www.skillsforaustralia.com/cross-sector-projects/cyber-security/

7. Education and awareness - A behavioural approach to cyber security

We are aware that the Government is doing many activities in order to raise awareness across Australia - at individual and business/organisation levels - emphasising why good cyber hygiene is so important and suggestions on what to do to keep safe. The 2019 Stay Smart Online week is a good example of this, focussed on 'Reversing the Threat' and empowering Australians to 'take control' of their online identity.

There are other mechanisms and initiatives in place to raise awareness of cyber threats and their impact, for example, SCAMwatch operated by the Australian Competition and Consumer Commission, and Schools Cyber Security Challenges supported by ACSC..

We agree that these campaigns are important to raise awareness in Australian community and amongst businesses and disclosure of complex cyber threats and incidents are still necessary. However, they alone are not sufficient to drive good consumer outcomes. Even with increased awareness, we still see undesired cyber behaviours e.g. clicking on the links, having weak passwords, ignoring warnings about potential malware infection etc. which results in suboptimal decision making and choices. Accordingly, knowledge and awareness needs to be increased in conjunction with other influencing strategies[7].

Governments, regulators and proactive organisations around the world are increasingly employing behavioural economics insights to improve and better understand customer and citizen behaviours. For example, 'Ideas42' is a not for profit design and consulting organisation that has been examining critical challenges in cyber security through the lens of behavioural science[8]. ASIC is committed to applying behavioural economics insights to identify consumer problems and to detect when firms take advantage of consumer biases as stated in ASIC Release15-059 (2015).

We believe the Federal Government has a role to play not only in providing a stable and peaceful online environment but also helping shape the agenda to use of a behavioural approach to digital/technology products and services design to manage cyber risks.

In this context, PwC recommends the following for Australian Government's consideration of influencing consumer choices at scale and adopting a behavioural approach to cyber security:

- Become an early adopter of using behavioural economics to have an impact on cyber security industry, identify scalable mechanisms to shift behaviour and influence choices and establish regulation that drives the conversation away from just raising awareness and communications;
- Ask the question of what are the desired cyber behaviours that the Australian Government would like to shift in consumers/entities/businesses when making choices to create a safe online and digital experience for Australian residents and visitors;
- With the agenda of creating a Smart City, using behavioural science to develop "nudges" that will enable and equip people to make optimal decisions to manage cyber risks;
- Use the objectives/desired state behaviours to undertake evidence-based studies about how people think (their mental models) and behave in the real world by working closely with the private sector that is well placed to contribute to discussions on the practicality of solutions, and champion their implementation. Examples could include:
    - Exploring and testing a way to provide 'Cyber Security/Safety Star rating' on various mobile applications, products and URLs etc. for consumers to make more informed choices in that moment of decision making.

[7] Global Cyber Security Capacity Centre: Draft Working Paper: https://discovery.ucl.ac.uk/id/eprint/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf

[8] Supported by the William and Flora Hewlett Foundation Cyber Initiative in partnership with New America's Cybersecurity Initiative

There could be multiple hypotheses that can be established and tested to see what approach works best to complement awareness initiatives;

- Working with industry partners and companies to design products and services that 'introduce friction or extra steps' in a process e.g. malware or infection warnings could leverage this insight by adding additional steps to pass through them, such as requiring the user to confirm twice that they want to proceed, or requiring the user to wait for 30 seconds or a minute after clicking through a warning before they can proceed[9]; and,

- Assess 'demographic differences' (age, location, potential knowledge of computers/online platforms, access to online channels) and design strategies in alignment with various factors e.g. not all consumers and businesses would have access to stay smart online website and are part of the campaign.

[9] http://www.ideas42.org/wp-content/uploads/2016/08/Deep-Thought-A-Cybersecurity-Story.pdf

8. Future challenges

There are a number of emerging technologies that are poised to fundamentally re-shape the future of cyber security as we know it. Whilst not an exhaustive list, we believe the promise of Quantum Computing and Artificial Intelligence represent potentially the two most influential in this category. Whilst these topics go well beyond cyber security, the 2020 Cyber Strategy has the opportunity to demonstrate the Government's forward-thinking approach to securing future technologies, as well as stimulating discussion across industry and academia to ensure these technologies continue to develop with security and safety in mind.

Australia is already on the forefront of Quantum Computing research, with the University of New South Wales regularly gaining global recognition on advances in the field, and many other academic institutions and private organisations also contributing to research and the development of products.

While much of the mainstream media with respect to quantum computing focuses on doomsday scenarios where all current encryption methods could be made redundant, the reality is quite different. Quantum computing will not make all current computers obsolete, nor will it make all current encryption methods obsolete. They will however likely fulfil specific purposes where they can outperform classical computers by orders of magnitude, and as with any technology leap with this sort of promise, close attention is being paid by governments and militaries to understand its true potential. It is important that Australia continues to maintain its position as a global leader in quantum computing research and application, which will require the ongoing support of Government to fund research, and drive collaboration across public and private sectors.

Artificial Intelligence is already changing the way organisations and consumers interact. Companies are using AI to automate tasks that humans used to do, such as fraud detection or vetting resumés and loan applications, thereby freeing those people up for higher level work. Doctors are using AI to diagnose some health conditions faster and more accurately. Chatbots are being used in place of customer service representatives to help customers address simple questions. With this tremendous potential comes a great responsibility - to ensure it used responsibly and ethically, which PwC has been a strong proponent of in recent times[10].

Similar to quantum computing, the Government needs to continue to foster innovation and collaboration so that Australia remains at the cutting edge of AI advancement. Our view is that Australia can and should take a proactive global leadership role with respect to the secure, responsible and ethical use of AI across the public and private sector. This will ensure that when AI technologies becomes more widely understood and adopted by the general Australian public, it is based on a foundation of trust already established by Government.

Throughout this paper we have emphasised that technology is only one aspect of cyber security, and the need for more human-centric approaches to strengthening the cyber resilience of our nation. No platform embodies this challenge more than the prospect of artificial intelligence - where our technology prowess and human behaviour will converge to create a powerful ally, and potentially even greater adversary.

[10] https://www.pwc.com/gx/en/issues/data-and-analytics/artificial-intelligence/what-is-responsible-ai/responsible-ai-practical-guide.pdf

www.pwc.com.au