Australia's 2020 Cyber Security Strategy

Industry Advisory Panel Report

Contact us

Enquiries regarding the licence and any use of this document are welcome at:
Cyber, Digital and Technology Policy Division
Department of Home Affairs
4 National Circuit Barton ACT 2600

cybersecuritystrategy@homeaffairs.gov.au

P - 20-02329

Australia's 2020
Cyber Security Strategy

Industry Advisory Panel Report

July 2020

Table of Contents

Executive Summary

Technology now sits at the very heart of the lives of most Australians and increasingly shapes our economy, our society and our future. It is fast changing how we live, learn and work as well as creating incredible new opportunities, efficiencies and benefits – from remote working to digitised global supply chains, from tele-health to e-commerce.

The Federal Government is clear-eyed about the opportunities:

> *"Our Government's goal is for Australia to be a leading digital economy by 2030. Our degree of success will be critical to income growth and job creation over the next decade and beyond. Our extensive policy agenda encompasses digital access, connectivity, consumer data and competition policy, government service delivery and skills development, trade and global e-commerce governance, as well as the necessary focus on security and privacy concerns."*
>
> **Prime Minister Scott Morrison**
> BCA annual dinner keynote
> 21 November 2019

The scope and timing of that ambition is well placed. As we enter the 2020s the world is on the exciting cusp of a fourth industrial revolution driven by connectivity and digital technologies.

Artificial intelligence, sensors, autonomous machines and systems, edge compute, augmented reality and 5G will combine to create incredible new products and services, infuse the physical world with digital, revolutionise business operations, elevate human work, and serve customers and citizens in many new ways.

All of this was true before the emergence of the COVID pandemic which has only further underlined the importance of the digital economy in Australia. In responding to COVID, mandatory social distancing and self-isolation means healthcare, education, work and commerce and even staying in touch with friends and family are largely being done online. Looking beyond this crisis, technology and our ability and willingness to embrace the digital world has now emerged as central to a rapid economic recovery.

With so much at stake, robust and effective cyber security has never been more important and the 2020 Cyber Security Strategy Industry Advisory Panel welcomed the opportunity to contribute to that outcome.

The Panel were engaged in late 2019 at a time when the Federal Government were reviewing the progress of the landmark 2016 Cyber Security Strategy. This work led to the establishment of the Joint Cyber Security Centres, creation of cyber.gov.au as a one-stop-shop for cyber security advice and the establishment of key leadership positions including the Ambassador for Cyber Affairs.

Despite these achievements the Government acknowledged that significant and ongoing changes in the scope, scale and sophistication of cyber threats required an evolution in our approach to cyber security as a nation.

Minister for Home Affairs, Peter Dutton, has described how meeting the evolving cyber challenge is key to Australia's economic prosperity and national security. In September 2019 he said: *"Cyber security has never been more important to Australia's economic prosperity and national security. In 2016, the Australian Government delivered its landmark Cyber Security Strategy, which invested $230 million to foster a safer internet for all Australians. Despite making strong progress against the goals set in 2016, the threat environment has changed significantly and we need to adapt our approach to improve the security of business and the community."*

"Cyber criminals are more abundant and better resourced, state actors have become more sophisticated and emboldened, and more of our economy is connecting online. Cyber security incidents have been estimated to cost Australian businesses up to $29 billion per year and cybercrime affected almost one in three Australian adults in 2018."

This escalation in malicious cyber activity has only increased during COVID as we have been forced to work, learn and connect from home, outside of some of our usual security frameworks. We are seeing malicious actors including criminals and state based actors exploiting this opportunity to their own advantage, to the significant risk and detriment of Australian citizens.

On 30 June 2020, Prime Minister Scott Morrison pointed to the urgency of the issue: *"The Federal Government's top priority is protecting our nation's economy, national security and sovereignty. Malicious cyber activity undermines that."*

Australia's ability to prosper as a digital economy can be enhanced if we increase our investment in our cyber defences. We must move to comprehensively protect ourselves and our businesses from cybercrime, protect our national infrastructure and improve the security of our institutions – including our democratic electoral processes, which have been the subject of malicious cyber-attack in other parts of the world. It is crucial we act quickly and decisively.

The 2020 Cyber Security Strategy Industry Advisory Panel was formed in November 2019 and asked to provide advice from an industry perspective on best practices in cyber security and related fields; emerging cyber security trends and threats; key strategic priorities for the 2020 Cyber Security Strategy; significant obstacles and barriers for the delivery of the 2020 Cyber Security Strategy; and the effect of proposed initiatives on different elements of the economy, both domestic and international.

The Panel met 13 times between November 2019 and July 2020, including two meetings with Minister Dutton and formal briefings, including some classified, from the Department of Home Affairs, the Australian Signals Directorate, the Attorney-General's Department, the Department of the Treasury, the Australian Competition and Consumer Commission, the then Department of Communications and the Arts, the eSafety Commissioner, the Australian Federal Police, the Australian Security Intelligence Organisation, the Cyber Security Cooperative Research Centre and AustCyber.

After broad consultation and careful deliberation, the 2020 Cyber Security Strategy Industry Advisory Panel has developed a series of recommendations that we believe strike the right balance between increasing our cyber defences, promoting the development of a digital economy and countering threats to our economy, safety, sovereignty and national security.

The Panel's recommendations are structured around a framework with five key pillars:

- **Deterrence:** deterring malicious actors from targeting Australia.
- **Prevention:** preventing people and sectors in Australia from being compromised online.
- **Detection:** identifying and responding quickly to cyber security threats.
- **Resilience:** minimising the impact of cyber security incidents.
- **Investment:** investing in essential cyber security enablers.

On deterrence, we recommend that the Government establish clear consequences for those targeting Australia and people living in Australia. A key priority is increasing transparency on Government investigative activity with more frequent attribution and consequences applied where appropriate. Strengthening the Australian Cyber Security Centre's ability to disrupt cyber criminals by targeting the proceeds of cybercrime derived both domestically and internationally is a priority.

On prevention, the recommendations include the pursuit of initiatives that make businesses and citizens in Australia harder to compromise online. This includes a clear definition for critical infrastructure and systems of national significance with a view to capturing all essential services and functions in the public and private sectors; consistent, principles-based regulatory requirements to implement reasonable protection against cyber threats for owners and operators of critical infrastructure and systems of national significance; measures to build trust in technology markets through transparency such as product labelling; and the extension of existing legislative and regulatory frameworks relevant in the physical world to the online world. Ultimately cybercrime is just crime, cyber espionage is just espionage and hacktivism is just activism online.

All levels of Government should take steps to better protect public sector networks from cyber security threats. Government agencies should be required to achieve the same or higher levels of protection as privately-owned critical infrastructure operators. Different levels of government should collaborate to share best practices and lessons learned. Ultimately Governments should be exemplars of cyber security best practice and Australian governments have some way to go in achieving this aspiration.

On detection, recommendations include that Government establish automated, real-time and bi-directional threat sharing mechanisms between industry and Government, beginning with critical infrastructure sectors. Government should also empower industry to automatically block a greater proportion of known cyber security threats in real-time including initiatives such as 'cleaner pipes'.

On resilience, recommendations include the development of proactive mitigation strategies and strengthening of systems essential for end-to-end resilience. Government should strengthen the incident response and victim support options already in place. Speed is key when it comes to recovering from cyber incidents and Government should hold regular large scale and cross-sectoral cyber security incident response exercises to improve the readiness of interdependent critical infrastructure providers and government agencies.

Resilience includes both the ability to recover from a cyber-attack as well as the redundancy designed-in to systems and processes. In other words, a key factor influencing the ability to recover is the level of redundancy present in systems in the first place.

It is important to also call out that a number of recommendations to build resilience relate to the role of the individual, in particular around building cyber awareness. In this regard there is an important distinction between cyber security (which means protecting data and information networks and critical infrastructure functions) and cyber safety (which means protecting users from

harmful online content). The fundamental ability to participate safely online is the difference between enjoying the internet's abundant information resources and opportunities, and being a potential victim of a cybercrime.

On investment, recommendations support the ongoing development of highly specialised and effective capabilities exemplified by the Australian Cyber Security Centre and the state-based Joint Cyber Security Centres. This existing capability should be substantially increased and enhanced through significant investment and a more integrated governance structure that maintains an industry leadership role. It is going to be a critical enabler to the success of the 2020 Cyber Security Strategy.

The Panel is also of the view that it is important for Government and industry to continue to invest in cyber skills development and security risk management in Australia. Good enterprise security management includes all aspects of securing people, property and technology. This skills investment is recommended at both a professional and specialist skills level and also more broadly, and should include primary, secondary and tertiary courses (including programs that focus on all aspects of enterprise security risk management, particularly cyber skills uplift). Importantly many of these skills should be built as foundational requirements in science, maths, engineering and technology. Although the cyber skills and awareness of directors on the boards of Australia's listed companies has been developed in recent years, there is opportunity for further development and support.

Within this framework of 60 recommendations sit 25 high priority and 35 other recommendations that address the full spectrum of cyber security threats – from the 'routine' threats that target vulnerable people in Australia every day to sophisticated 'state actor' cyber-attacks that threaten our economy, safety, sovereignty and national security. The Panel recommends that threats to critical infrastructure, digital supply chains and systems of national significance should be addressed first.

State, territory and local governments should also be considered key implementation partners for all elements of the Strategy.

We encourage the Australian Government to establish formal mechanisms to ensure ongoing engagement with all levels of government.

Clear roles and responsibilities

Cyber threats continue to shift and evolve and, as the threats evolve, so must our response. The recommendations we propose are built around creating robust and adaptable defences as threats emerge and technologies and opportunities change.

It is important to recognise that effective cyber defences involve more than just investment dollars. Our report highlights that an effective response includes fundamentally organising and governing differently to ensure more efficient and effective use of resources and aligning cyber security imperatives across Australia.

This requires clearly defined roles, responsibilities and authorities to be established and the Federal Government's role in leading and coordinating the national effort is therefore critical. Ultimately the Government is in a unique position with access to information and tools which mean that in particular circumstances it is the appropriate party to lead our cyber defence. This is not only about the Federal Government but effective coordination with other tiers of Government. Government also plays an important role partnering with industry, as well as broadening community awareness and skills in adequately addressing cyber issues.

If Australia's cyber security is well organised and well governed then the application of all resources - public, private, people, infrastructure and capital investment – will achieve far more efficient and effective results. This was an important learning from the 2016 Cyber Strategy.

The only way to look at cyber security is as a team. Large enterprises, small and medium businesses and Government all have shared platforms, common customers, and all are the target of attacks. We all therefore play a role, and share an accountability, in keeping Australians safe.

Implementation

The 2020 Strategy will be largely measured based on how well it is implemented and whether it meets or exceeds objective and bold metrics. During consultation, some stakeholders viewed implementation of the 2016 Cyber Security Strategy as being limited by regular changes in governance arrangements, lack of clarity about the roles of different government departments and inconsistent public communication.

We encourage the Government to create strong governance and evaluation mechanisms around the 2020 Strategy. Data collection and evaluation, based on a maturity framework, should be afforded a high priority.

A standing industry advisory panel could be established to advise the Minister for Home Affairs on cyber security matters and implementation of the 2020 Strategy on an ongoing basis strengthening the important link between Government and industry. Such a panel should have appropriate representation from across business, academia and the community.

State and territory governments should be closely involved in implementation of the Strategy. It would be appropriate for state and territories to be represented on the public service committee responsible for implementing the Strategy.

Never a more important time

The Australian Government deserves real credit for the leadership it has shown on cyber security, including through the development of Australia's 2020 Cyber Security Strategy and the announcement of a $1.35 billion investment (Cyber Enhanced Situational Awareness and Response package) over the next 10 years which will support a number of the key recommendations set out in this report. With robust cyber security critical for our economic prosperity, international competitiveness and national security, this work will only become more important as Australia continues to digitise in the future.

The Chair of the Panel, Andy Penn, describes the opportunity and the challenge ahead:

"The beginning of the 2020s has been marked by a period of profound disruption for Australia with the devastating bushfires and the COVID virus. At the same time and as we progress further into the decade we will also experience an extraordinary new era of technology innovation. As an optimist I am convinced we will adapt and technology will help to solve some of society's biggest challenges and realise some of its biggest opportunities.

But at the same time, this period of working and studying from home and the accelerated trend to a digital economy are exposing us to a more vulnerable environment of cyber threats. We are seeing increased levels of malicious cyber activity both state based and criminal. Successfully meeting this challenge requires upgrading Australia's cyber defences to be strong, adaptive and built around a strategic framework that is coordinated, integrated and capable. The 2020 Cyber Security Strategy has an opportunity to be all of those things and provide an enormous – and never more important - contribution to a safer, more prosperous Australia."

The Panel appreciate the opportunity to have worked with the Australian Government to build Australia's cyber defences through the 2020 Cyber Security Strategy and look forward to the key initiatives emanating from this work - they could not arrive at a more important time.

List of Recommendations

Objective 1: There are clear consequences for targeting Australians

In considering how Australia can increase the consequences of malicious cyber activity for nation states and cyber criminals, the 2020 Cyber Security Strategy should as an immediate priority:

1. Target the growing volume of cybercrime by increasing operational-level cooperation with states, territories, and international partners leveraging the Australian Cyber Security Centre and Joint Cyber Security Centres.
2. Increase the Australian Cyber Security Centre's ability to disrupt cyber criminals on the Dark Web and to target the proceeds of cybercrime.
3. Leverage existing cybercrime awareness raising campaigns to better inform businesses and individuals about new and emerging cybercrime threats to them.
4. Hold malicious actors accountable via enhanced law enforcement, diplomatic means, and economic sanctions or otherwise as appropriate.
5. Work with industry to better inform threat visibility and Government attribution activities where appropriate.
6. The Australian Government should openly describe and advocate the actions it may take in response to a serious cyber security incident to deter malicious cyber actors from targeting Australia.
7. Promote international law and continue to embed norms of responsible state behaviour online, in particular those that relate to the protection of critical infrastructure serving the public and deterring malicious cyber activity including intellectual property theft and ransomware attacks.

Objective 2: Cyber risks are owned by those best placed to manage them

In considering how Australia can improve cyber security risk management across the economy and for critical infrastructure, the 2020 Cyber Security Strategy should as an immediate priority:

8 Review the Australian Government's definition for critical infrastructure with a view to capturing all essential systems and functions in the public and private sectors and supply chains, including digital infrastructure such as data centres, that address all systems of national significance.

9 Introduce consistent, principles-based requirements to implement reasonable protection against cyber threats (where needed) for owners and operators of critical infrastructure (regardless of whether owned or operated by Government or private), with measurement based on a fit-for-purpose cyber maturity-based framework. In alignment with international best practice, this should leverage rather than duplicate existing sectoral regulations and minimise regulatory burden.

We further recommend that the 2020 Cyber Security Strategy should:

10 Review Australia's legislative environment for cyber security to ensure that suppliers of digital products and services have appropriate obligations to protect their customers.

11 Strongly encourage major vendors to sign-up to a voluntary 'secure by design' charter to leverage international best practice.

Objective 3: Australians practise safe behaviours at home and at work

In considering how Australia can reduce human risk factors in cyber security, the 2020 Cyber Security Strategy should as an immediate priority:

12 Unify all Government messaging on online safety and cyber security awareness raising, noting that existing campaigns run by different Government agencies share a common audience who do not distinguish between different online issues. Government should speak with one voice. Campaigns should be age and sector appropriate.

13 Increase assistance to small and medium businesses and the community through cyber security toolkits, trusted advice and practical assistance.

We further recommend that the 2020 Cyber Security Strategy should:

14 Partner with industry to increase the scale, reach and impact/effectiveness of cyber security awareness raising campaigns, including through co-design and co-funding where appropriate.

15 Incentivise large businesses to provide cyber security support to small and medium businesses in their supply chain and customer base.

Objective 4: Government is a cyber security exemplar

In considering how the Australian Government can improve trust in the cyber security of its own systems and networks, the 2020 Cyber Security Strategy should as an immediate priority:

16 Make Australian governments exemplars of enterprise security risk management, including cyber security, physical security and personnel security.

17. Require Government agencies providing essential services to meet the same cyber security standards as privately owned critical infrastructure, with increased accountability and oversight.

18 Prioritise the decommissioning or hardening of vulnerable legacy systems as part of an accelerated shift towards secure cloud based services.

We further recommend that the 2020 Cyber Security Strategy should:

19 Better coordinate digital procurement decisions across Government, with a view to negotiating best practice outcomes and where appropriate cost savings with common vendors.

20 Leverage Government procurement processes to improve cyber security through purchasing products and services with higher standards.

21 Require larger, more capable Government departments to provide cyber security services to smaller agencies on a basis that is uniform, consistent and risk based.

22 Fund the Australian Cyber Security Centre (ACSC) to continue its rolling program of cyber security improvements (but not audits) for other Australian Government agencies. Given the ACSC essentially provides a second line of defence role in risk management terminology, audit should be undertaken by a separate agency.

Objective 5: Trusted goods, services and supply chains

In considering how Australia can encourage the development of a digital technology market where security is built-in across the supply chain, the 2020 Cyber Security Strategy should as an immediate priority:

23 Increase investment in cyber security research and development, including basic sciences, and coordinate state and territory-led research and development at the national level. This will enable Government to maximise economic opportunities and drive national security outcomes.

24 Work with industry to increase Australia's role in shaping international cyber security standards.

25 Work with industry and likeminded nations to encourage diversity, transparency and competition in digital supply chains.

We further recommend that the 2020 Cyber Security Strategy should:

26 Develop a program to identify and assess emerging threats and emerging technologies that could introduce new vulnerabilities leveraging Australia's global leadership in policy development related to cyber risks. The CSIRO and Defence Science and Technology are two existing national agencies that could be leveraged to support the development of this program.

27 Obtain industry consensus around what cyber security standards should be used in Australia and accelerate the adoption of these standards to ensure digital products and services are 'secure by design'.

28 Require increased recognition and adoption of specific cyber security standards in Australia.

29 Implement a dynamic accreditation or mandatory cyber security labelling scheme so that consumers can make informed choices about their own cyber security (recognising that accreditations and product labelling will need to take account of changes in technology).

30 Work with the emerging cyber insurance industry to improve access to reliable actuarial data and develop best practice approaches to nudging the cyber security hygiene of policy holders.

31 Build transparency into critical and emerging technology supply chains to enable consumers to trust the cyber security of their devices.

32 Consider mandatory requirements or certification of supply chains for software and hardware supporting critical infrastructure.

Objective 6: Comprehensive situational awareness enables action

In considering how the Government and industry can improve the timeliness and quality of threat information sharing to better anticipate and respond to threats, the 2020 Cyber Security Strategy should as an immediate priority:

33 Establish automated, real-time and bi-directional threat sharing mechanisms between Government and industry, beginning with critical infrastructure sectors.

We further recommend that the 2020 Cyber Security Strategy should:

34 Empower industry to automatically block a greater proportion of known cyber security threats in real-time, including by providing legislative certainty.

35. Consider the development of 'safe harbour' legislative provisions that give industry certainty about the information it can voluntarily share with other organisations to prevent or respond to cyber security threats.

36. Resume the publication of annual reports on the state of cyber security threats to Australia.

Objective 7: Effective incident response options and victim support

In considering how Government and industry can create and sustain a high level of preparedness for incidents and improve support to victims, the 2020 Cyber Security Strategy should as an immediate priority:

37 Map in partnership with industry, the resilience of critical infrastructure networks, with a view to increasing maturity levels over time.

38 Identify and assess in partnership with industry interdependencies, single points of failure and consolidation risk to enable better understanding of cyber risk.

39 Work with industry to agree a unique set of circumstances in relation to critical infrastructure and systems of national significance where it would be necessary for Government to provide reasonable assistance to Australian businesses during a cyber security emergency, and define suitable oversight and thresholds for action.

40 Provide additional funding to not-for-profit organisations that support victims of cybercrime and communicate their role and existence to the community.

We further recommend that the 2020 Cyber Security Strategy should:

41 Hold a large scale and cross-sectoral cyber security incident response exercise at least every two years to improve national coordination and incident response readiness of interdependent critical infrastructure providers and government agencies. Exercises should include links to international activities where appropriate.

42. Include industry in Australia's formal incident response plans by amending the national Cyber Incident Management Arrangements.

Enabler 1: The Australian Signals Directorate's Joint Cyber Security Centres (JCSCs)

Recognising the JCSCs are the local offices of the Australian Cyber Security Centre, the 2020 Cyber Security Strategy should as an immediate priority:

43 Establish a national board chaired by ASD (with industry co-chair) and including industry representation to strengthen the strategic leadership of the Joint Cyber Security Centres, underpinned by a charter outlining the JCSCs' scope and deliverables.

44 Fund ASD to provide enhanced technical and consulting cyber services to industry through the JCSC Program, including a greater focus on information sharing.

We further recommend that the 2020 Cyber Security Strategy should:

45 Create a staff exchange program between the ACSC, academia and industry to enable cross-sectoral collaboration and information sharing. The CSIRO and Defence Science and Technology could be leveraged to support the engagement between academia and industry.

46 Dedicate additional JCSC resources to engage with local governments.

Enabler 2: Cyber security skills

In considering how Government, industry and academia improve risk postures by strengthening the pipeline of skilled cyber security professionals, the 2020 Cyber Security Strategy should:

47 Position the Australian Government to take a national leadership role in addressing Australia's cyber security skills shortage.

48 Work with professional bodies and academia to include cyber security education in adjunct technical fields such as engineering and data science and extend cyber skills training to company directors.

49 Consider creating an internationally aligned accreditation scheme to recognise the skills, experience and qualifications of cyber security professionals in both technical and management roles. This should including mapping the equivalency of existing qualifications.

50 Adopt a national framework that defines the roles that make up the cyber security profession. Use this framework to develop a national workforce planning program for the cyber security profession.

51 Consider additional incentives to attract and retain Government cyber security specialists.

52 Strengthen voluntary professional accreditation of university cyber security courses, to provide greater assurance to students and employers that courses are meeting contemporary industry demands.

53 Develop targeted cyber security programs in primary and high school to inspire young people to take up a career in cyber security, and build foundational skills in science, maths, engineering and technology.

54 Undertake a regular survey across Government and business to better understand the size of cyber security skills shortage in Australia and evaluate new programs under the 2020 Cyber Security Strategy.

Enabler 3: Intelligence and Assessment

The Panel recognises the importance of intelligence-led efforts to combat malicious cyber activity and acknowledges that this is primarily a matter for Government. The Panel is of the view that successful implementation of the recommendations above relating to Objective 1 (Clear consequences for targeting Australia and Australians), Objective 6 (Comprehensive situational awareness enables action) and Enabler 1 (The Australian Signals Directorate's Joint Cyber Security Centres) will support Government to enhance the delivery of this enabler.

The Panel encourages the Government to be open and transparent about its knowledge of the threat environment wherever possible, including by declassifying information when appropriate, increasing proactive cyber threat briefings to security cleared industry personnel with a need to know, and sponsoring greater numbers of industry representatives to obtain security clearances.

Enabler 4: Governance

In considering how Government should manage implementation of the Strategy, including oversight arrangements, ongoing industry consultation and reporting mechanisms, the 2020 Cyber Security Strategy should as an immediate priority:

55 Include state and territory Governments in development, implementation and monitoring of all relevant initiatives under the 2020 Cyber Security Strategy.

We further recommend that the 2020 Cyber Security Strategy should:

56 Appoint an industry advisory panel to advise the Government on cyber security on an ongoing basis, including on the implementation of the 2020 Cyber Security Strategy. The panel should work with the accountable Government agency or department responsible for implementing the Strategy, while reporting to the Minister for Home Affairs.

57 Task the industry advisory panel to publish an annual progress report on implementation of the 2020 Cyber Security Strategy and emerging cyber security threats and priorities for Australia from an industry perspective.

Enabler 5: Evidence and Evaluation

In considering the best practice approaches to evidence collection and evaluation that can inform implementation of the Strategy and future policy making, the 2020 Cyber Security Strategy should:

58 Adopt a maturity model approach to evidence and evaluation.

59 Invest in improved data collection, research and analysis to underpin evaluation of the performance against the metrics of the 2020 Cyber Security Strategy. This should include periodic surveys of the cyber security maturity of public and private sector organisations.

60 Publish regular updates on implementation of the 2020 Cyber Security Strategy and periodically review and refresh the Strategy every 2 or 4 years.

Process

On 6 September 2019, the Australian Government announced that it would develop a 2020 Cyber Security Strategy as part of its commitment to protect Australians from cyber security threats.

On 25 November 2019, the Minister for Home Affairs announced the establishment of the Industry Advisory Panel to provide strategic advice to support the development of Australia's 2020 Cyber Security Strategy. The role of the Panel was advisory only and comprised:

- Mr Andrew Penn, CEO and Managing Director, Telstra (Chair);
- Secretary Kirstjen Nielsen, former US Secretary of Homeland Security (appointed 18 December 2019 to provide the Panel with international expertise and perspectives);
- Mr Robert Mansfield AO, Chair of Vocus Group;
- Ms Robyn Denholm, Chair of Tesla;
- Mr Chris Deeble AO CSC, Chief Executive of Northrop Grumman Australia; and
- Mr Darren Kane, Chief Security Officer NBN Co.

Further details on the Panel members are at Appendix 2.

The Panel's Terms of Reference are at Appendix 1. The Panel were advised that the 2020 Cyber Security Strategy will seek to:

- protect and secure nationally significant infrastructure, systems and data;
- ensure cyber-risk is managed appropriately in the economy and community;
- improve assistance and support to individuals, families and small businesses;
- build a mature and trusted domestic market for secure technologies, products, services and professionals;
- create new ways for businesses and individuals to prosper in the digital age; and
- strengthen our cyber security capability.

The Panel were asked to provide advice on:

- best practices in cyber security and related fields;
- emerging cyber security trends and threats;
- key strategic priorities for the 2020 Cyber Security Strategy;
- significant obstacles and barriers for the delivery of the 2020 Cyber Security Strategy; and
- the effect of proposed initiatives on different elements of the economy, both domestic and international.

The Panel met 13 times between November 2019 and July 2020, which included two meetings with the Minister. The Panel structured its deliberations around 12 problem statements prepared by the secretariat (at Appendix 3) that reflected the key themes that stakeholders raised during the public consultation process. The Panel received formal briefings from the Department of Home Affairs, the Australian Signals Directorate, the Attorney-General's Department, the Department of the Treasury, the Australian Competition and Consumer Commission, the then Department of Communications and the Arts, the eSafety Commissioner, the Australian Federal Police, and the Australian Security Intelligence Organisation.

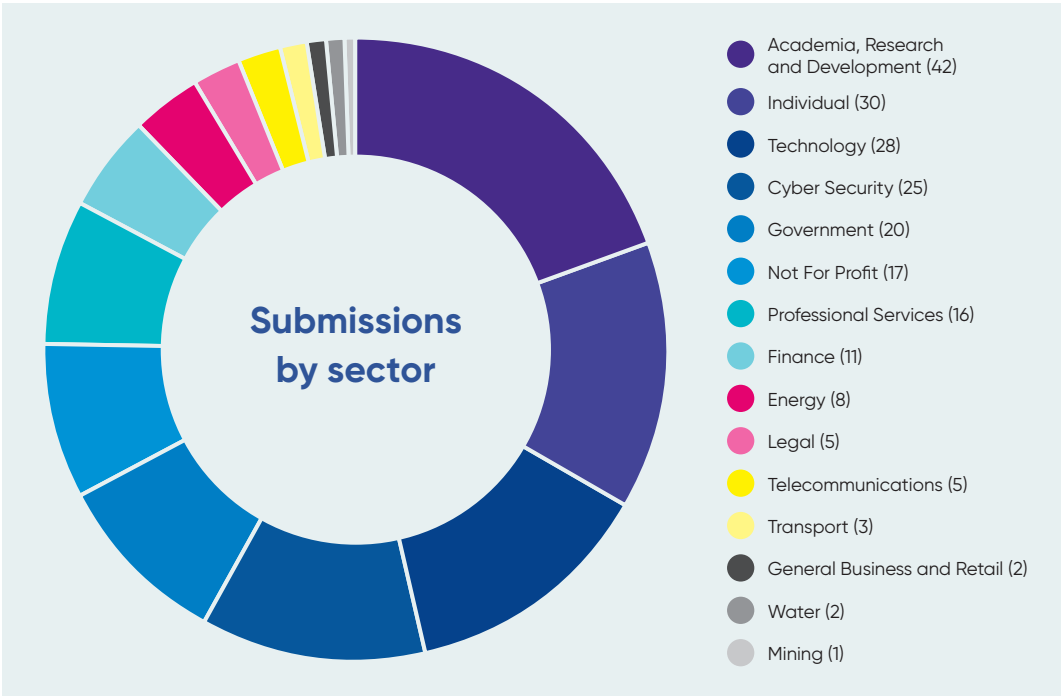
The Department of Home Affairs provided a secretariat function for the Panel.

Stakeholder engagement

The Panel's deliberations were informed by two rounds of stakeholder consultation conducted by the Department of Home Affairs between September 2019 and February 2020. The Panel also independently consulted senior leaders in small, medium and large businesses, government, peak industry groups, and other interested stakeholders.

A public discussion paper posted to the Department of Home Affairs website on 6 September 2019 was downloaded more than 2,500 times while submissions were open. Home Affairs received a total of 215 submissions, 156 of which were public and made available to the Panel. The remainder were confidential and were not provided to the Panel. A wide range of stakeholders made submissions, including cyber security companies; critical infrastructure providers; small, medium and large businesses; state, territory and local governments; legal experts; consumer and other advocacy groups; and academia (see Figure 1 below).

Figure 1: Written submissions by sector



More than 1,400 people took part in consultation events held by Home Affairs in each state and territory. These included 19 open forums, six critical infrastructure roundtables, meetings with the industry leadership of the Joint Cyber Security Centres, roundtables with state and territory governments, and over 50 bilateral meetings. Home Affairs also held a range of dedicated forums with small businesses, large technology companies, academia, local governments and the defence industry.

Further information on the consultation process is available from:
www.homeaffairs.gov.au/cybersecurity

Current threat environment

The Australian Signals Directorate provided the Panel with regular updates on the threat environment. Malicious cyber activity against Australia is increasing in frequency, scale and sophistication with cyber adversaries constantly developing their tools and tradecraft to circumvent the ability of organisations, including governments, to detect and defend against sophisticated cyber threats.

Australia continues to be a target of persistent and targeted cyber espionage and the number of states who have acquired or are acquiring cyber espionage capabilities is increasing. Over the past 12 months, the Australian Cyber Security Centre (ACSC) has responded to activity against all levels of government, industry, health, businesses and the academic sector.

Sophisticated state-based actors seek to compromise networks to obtain economic, foreign policy, health, defence and security information for strategic or economic advantage. These actors are typically the most sophisticated and persistent form of adversary, posing a significant threat to Australia's economy, safety, sovereignty and national security.

While Advanced Persistent Threats can use very sophisticated tools and tradecraft against well secured targets they more often than not use basic tradecraft – like sending a phishing email – because basic techniques still deliver results. Many successful compromises continue to occur through the use of publicly available tools targeting known vulnerabilities which have not been patched or otherwise mitigated by the victim.

Cybercrime is also a pervasive and endemic threat and the most significant threat in terms of overall volume costing Australians and Australian businesses billions of dollars each year. Cybercriminals have proven themselves to be flexible and inventive, and as the complexity, sophistication and impact of cybercrime continues to evolve, cybercrime activity is likely to increase.

Of particular concern are transnational cybercrime syndicates and their affiliates, who develop, share, sell and use increasingly sophisticated tools and techniques. There's a booming underground marketplace offering cybercrime-as-a-service, or access to high-end hacking tools that were once only available to nation states.

Cybercriminals operate at scale with the principle of quantity over quality. They usually target individuals and organisations by exploiting particular technological vulnerabilities. The ACSC expects to see more business email compromises, cryptocurrency mining, credential harvesting and ransomware. Ransomware is a particularly grave threat because it disrupts the operations of businesses and governments by encrypting files and demanding a ransom for their return. Recovering from such incidents is almost impossible without comprehensive backups.

Our vision, framework and recommended outcomes

The Panel shares the view that the Minister for Home Affairs expressed at the first meeting of the Panel on 25 November 2019: there is an urgent need for Australia to step up its cyber defences. A changing threat environment and the evolving nature of technology means that there has never been a more important time for Government and industry to work together to strengthen Australia's cyber security settings. We need to address both highly sophisticated threats targeting critical networks and lower sophistication activities targeting vulnerable groups such as small businesses and families.

Internet connected devices deliver our power and water, help transport people and goods, process our personal information, predict which crops will succeed, monitor our health, help our children learn, and keep us entertained and informed. We are now reliant more than ever on the internet to work and study from home and make meaningful social connections. Unfortunately, many malicious actors have sought to exploit reliance on the internet for their own financial and strategic benefit.

The briefings we received from Australia's national security and law enforcement agencies made it clear that Australia faces growth in malicious cybercrime. One in three Australian adults has been a victim of cybercrime, such as fraud, identity theft and malware. [1]

Rates of cybercrime are growing because it is cheap and easy, relative to the potential gains. We now find ourselves in a world where many of the consequences of cyber risk are shouldered by those in our community that are the least well equipped to deal with them.

Improving cyber security at the personal, commercial and national level is a complicated task. Technological advancement is now so rapid that it is almost impossible to forecast what the cyber landscape will look like in the coming years, let alone the coming decades. Cyber threats are a global problem and we are connected, politically and technologically to the actions of the rest of the world. At the same time, global supply chain for key strategic technologies such as 5G are becoming concentrated and dominated by a small number of global players and producers. Focus on technology supply chain diversification and R&D should be a key aim for government, in partnership with industry.

1 Norton 2019, Norton LifeLock Cyber Security Insights Report 2018 – Australia

Our vision

The Panel developed a vision that guided it during its deliberations - strong cyber security enables Australians to prosper. In preparing its framework, suggested outcomes and recommendations, the Panel has endeavoured to strike the balance through this vision between realising the opportunities that a cyber safe and secure economy presents Australia, and countering threats to our economy, safety, sovereignty and national security.

Our framework

Our recommended framework for the 2020 Cyber Security Strategy is illustrated at Figure 2. We intend this framework to be relevant to the full spectrum of cyber security threats – from the 'routine' threats that target vulnerable people in Australia every day, to sophisticated threats that threaten our economy, safety, sovereignty and national security.

Figure 2: 2020 Cyber Security Framework

Outcomes

Our recommended outcomes for the Strategy are:

- **Deterrence** - deterring malicious actors from targeting Australia.
- **Prevention** - preventing people and sectors in Australia from being compromised online.
- **Detection** - identifying and responding quickly to cyber security threats.
- **Resilience** - minimising the impact of cyber security incidents.
- **Investment** - investing in essential cyber security enablers.

These outcomes broadly align with well-known technical models for cyber security and should be intuitive for many cyber security practitioners. The recommended outcomes also have the advantage of being conceptually comprehensive and enduring, allowing the Strategy to adapt to an evolving threat environment.

Objectives

We recommend the Government adopt the following objectives as measurable steps towards achieving the proposed outcomes. These objectives are based on the key themes of stakeholder feedback under each outcome.

For deterrence:

1 There should be clear consequences for targeting Australians.

For prevention:

2 Cyber risks should be owned by those best placed to manage them.

3 Australians should practice safe behaviours at home and at work.

4 Government should be a cyber security exemplar.

5 Australians should have access to trusted goods, services and supply chains.

For detection:

6 Comprehensive situation awareness should enable action in response to threats.

For resilience:

7 Australia should have access to effective response options and victim support.

For investment:

8 Government and industry to mature their collaboration through Australian Signals Directorate's Joint Cyber Security Centres.

9 The pipeline of skilled cyber security professionals should be strengthened and investment made to uplift cyber skills in Australia.

10 Government to increase investment in intelligence-led efforts and openly share threat information with industry.

11 Government is encouraged to appoint an external advisory panel to review the implementation of the Strategy led by the accountable Government agency or department.

12 The implementation of the Strategy should be based on a maturity framework that assesses performance against objective and bold metrics.

Roles and Responsibilities

The Panel recommends that the 2020 Cyber Security Strategy clarifies roles for Government, industry and individuals in the community as illustrated at Figure 3.

The Government's primary role should be to strategically manage the highest consequence threats and sophisticated attacks to Australia using its unique tools and capabilities with a focus on critical national infrastructure. The Panel considers that Government also has an opportunity to be an exemplar of cyber security best practice for the private sector by

strengthening the defences of its own systems by meeting the same cyber security best practice expectations as critical infrastructure owners and operators.

In relation to critical infrastructure and systems of national significance, Government has a dual role to govern and lead best practice management of risks and vulnerabilities of this network, as well as operating part of it. This requires an urgent maturity based assessment of the security preparedness of each element of the network (including Government) and then focusing initiatives to lift the most vulnerable components. This also requires Government to seize the opportunity to elevate the security of its own systems.

Government is taking significant steps towards meeting its aspiration for Australian to be a leading digital economy by 2030. This has been demonstrated through the initiatives delivered by Services Australia through the Digital Transformation Strategy and more recently with the digital capabilities that were promptly deployed to support businesses and people in Australia impacted by COVID-19 restrictions. The Panel supports the Government's goal of making all of its services available digitally by 2025 and demonstrated cyber security best practice will be key to building trust with the community to utilise these digital capabilities.

As Stuart Robert, Minister for Government Services, identified in his address to the Australian Information Industry Association on 29 November 2019, in *"order to transform government service delivery, we must harness everything that technology and data has to offer for the benefit of all Australians"*. Digital is more than just technology, it *"is about applying the best processes, culture, business models as well as technologies to respond to people's raised expectations"*.

In line with the recent Thodey Review of the Australian Public Service, the Panel believes there is an opportunity to clarify accountabilities and improve consistency of decision-making on cyber security within Government. There are also opportunities for Government to play a more strategic role in improving real-time understanding of cyber security threats so that they can be acted upon by all participants in the cyber security ecosystem.

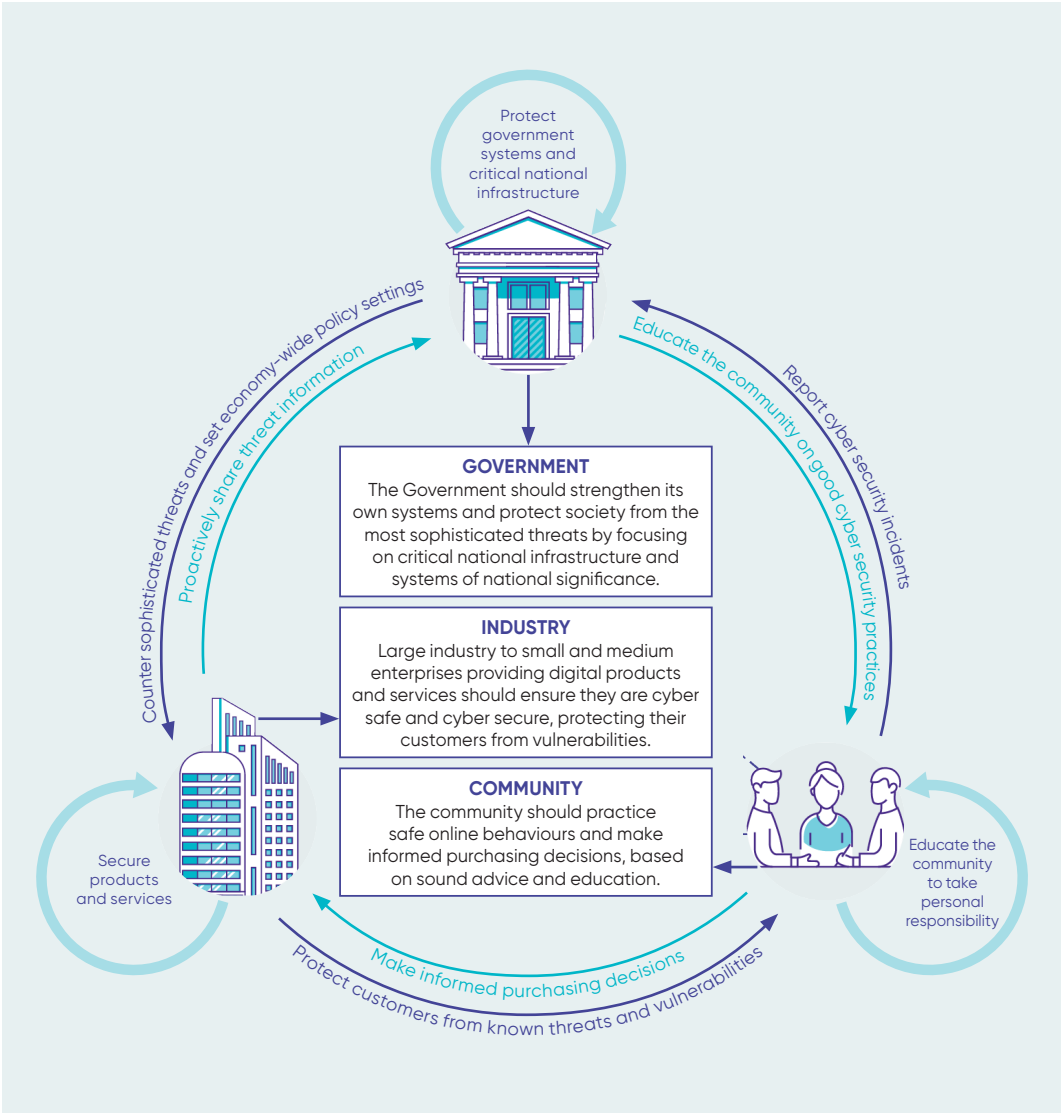
There is a need for Government and industry to focus on, and invest in, the development and maturity of the cyber security industry in Australia to leverage the potential of this growth industry.

Government is encouraged to increase its investment (and investment by industry) in cyber security research and development and support the ecosystem of cyber security business, particularly in the startup sector (such as further supporting the work of AustCyber that was established in 2017 and funded by the Government pursuant to the 2016 Cyber Security Strategy as a key enabler for cyber security research and development, as well as innovation). Australia is unlikely to be able to address key supply chain risks, including concentration risk, alone but can play an important role in supporting primary research in key basic services and the cyber ecosystem more generally.

The primary role for industry should be to grow its cyber security capabilities so that it can better protect a larger number of businesses and households. Providers of digital products and services should be increasingly responsible for ensuring they are cyber safe and secure protecting their customers from foreseeable cyber security harm and responsibly participate in a trusted cyber security marketplace.

Finally, the community should ultimately be responsible for keeping themselves safe online and making informed buying decisions which means improving awareness and education of cyber safe behaviours and practice. To support this Government should focus on awareness and training such as cyber security skills, including improving individual awareness of the importance of knowing the value of their own data, where it is and how it is protected.

Figure 3 Cyber Security Roles and Responsibilities



Our recommendations

The Panel has carefully considered the submissions to the Strategy and endeavoured to assimilate different stakeholder representations along with our own expertise including in relation to technology, people and process elements of cyber security. The Panel also considered domestic and international impacts and risks of proposed initiatives.

Our recommendations are organised under the objectives of our proposed framework. When taken together, our recommendations are a road map to reshaping roles and responsibility in cyber security in Australia.

Implementation

As noted in the *Executive Summary*, the 2020 Strategy will be largely measured based on how well it is implemented and whether it meets or exceeds objective and bold metrics. The 2016 Cyber Security Strategy made significant achievements in key areas, but some stakeholders felt that its overall success was reduced by inconsistent implementation.

We encourage the Government to create strong governance and evaluation mechanisms around the 2020 Strategy. Data collection and evaluation, based on a maturity framework, should be afforded a high priority.

A standing industry advisory panel could be established to advise the Minister for Home Affairs on cyber security matters and implementation of the 2020 Strategy on an ongoing basis strengthening the important link between Government and industry. At the very least a progress report should be provided to Cabinet on an annual basis.

State and territory governments should be closely involved in implementation of the Strategy.

Issues and Conclusions

Objective 1: Clear consequences for targeting Australia and Australians

How can Australia increase the consequences of malicious cyber activity for nation states and cyber criminals?

Issues

Australian governments, businesses and individuals are being increasingly targeted by cyber criminals and nation states. Rates of fraud, data breaches and unauthorised intrusions are growing at an alarming pace because malicious cyber activity is low risk and high reward. It is the Panel's view that cybercrime is crime and therefore a posture consistent with that should be taken across all aspects of the communications of government, industry, individuals and law enforcement agencies. The relative wealth of Australia makes us a lucrative target for cyber criminals, as demonstrated by the recent high profile attacks. Recent incidents demonstrate that sophisticated state actors and their proxies continue to seek access to sensitive information.

The scope of this threat significantly broadens when you consider a nation state attack on critical infrastructure and systems of national significance in Australia. A debilitating attack to one element of our interconnected critical infrastructure network in Australia can have serious flow on effects to other elements of the network and upstream and downstream supply chains. From a disruption to delivery times for fresh food and vegetables, to prolonged delays in provisioning life saving equipment to corrupted medical data, negative consequences for Australians can flow directly from such an attack. Response times to recover can be variable and subject to the redundancy and resiliency of impacted elements of the network.

During its deliberations, the Panel received a classified briefing from national security and intelligence officials that confirmed the scale and severity of this problem. The Panel heard that law enforcement agencies are struggling with the challenges posed by policing a borderless crime, the Dark Web, and the sophisticated tools employed by domestic and international cyber actors. Crimes are often committed across multiple jurisdictions because it makes it harder to investigate and prosecute the perpetrators. Agencies also lack the resources to cope with the sheer volume of cybercrime affecting the Australian community. To illustrate the size of the problem, the Australian Cyber Security Centre's 24/7 Global Watch receives a phone call about a cybercrime incident every 10 minutes.

> *"Australia should target the profits of cyber criminals and take a stronger approach to confronting state based actors. Malicious actors will continue to target Australia until there are real consequences for bad behaviour"*
>
> **Kirstjen Nielsen**
> Former U.S Secretary of Homeland Security

During public consultation, many stakeholders spoke about the rising cost of cybercrime on businesses and individuals, calling on Government to do more to disrupt the cash flows of cybercriminals and play a leading role in deterring malicious state-based actors. There was a clear view that as long as risks are low and rewards are high, malicious activity will continue and malicious actors will continue to invest in sophisticated ways to evade law enforcement.

Our conclusions

The Panel views the rapidly increasing rate of cybercrime and its impact on countless families and businesses as a critical problem that demands a concerted effort from Government and increased resourcing.

The Panel recognises that a significant amount of work has gone into simplifying cybercrime reporting arrangements for the public, and has made separate recommendations about enhancing the support provided to victims of cybercrime. These restorative measures are crucial; however, we also advise Government to strengthen its cyber security capabilities by investing more heavily in specialised, cross-jurisdictional and multi-agency teams to disrupt and prosecute cyber criminals. New tools and capabilities are likely to be required to address criminal threats on the Dark Web. This should be complemented by an awareness raising campaign to educate potential victims about cybercrime threats.

Deterrence of state sponsored malicious activity is a complex issue that can have second order impacts. While Government should continue to respond to state sponsored incidents on a case-by-case basis, we recommend the Government adopt a more forward leaning posture on attribution and deterrence (including by increasing the frequency of attribution, and joint international attribution, where relevant and appropriate). The Panel also encourages the Government to use voluntarily provided industry data to inform attribution activities where appropriate and publicly describe the kinds of actions it may take in response to cyber security incidents. This should all occur against a backdrop of promoting and adhering to international law, building on the existing work of the Department of Foreign Affairs and Trade and Australia's Ambassador for Cyber Affairs.

Our recommendations

In considering how Australia can increase the consequences of malicious cyber activity for nation states and cyber criminals, the 2020 Cyber Security Strategy should as an immediate priority:

1. Target the growing volume of cybercrime by increasing operational-level cooperation with states, territories, and international partners leveraging the Australian Cyber Security Centre and Joint Cyber Security Centres.
2. Increase the Australian Cyber Security Centre's ability to disrupt cyber criminals on the Dark Web and to target the proceeds of cybercrime.
3. Leverage existing cybercrime awareness raising campaigns to better inform businesses and individuals about new and emerging cybercrime threats to them.
4. Hold malicious actors accountable via enhanced law enforcement, diplomatic means, and economic sanctions or otherwise as appropriate.

5 Work with industry to better inform threat visibility and Government attribution activities where appropriate.

6 The Australian Government should openly describe and advocate the actions it may take in response to a serious cyber security incident to deter malicious cyber actors from targeting Australia.

7 Promote international law and continue to embed norms of responsible state behaviour online, in particular those that relate to the protection of critical infrastructure serving the public and deterring malicious cyber activity including intellectual property theft and ransomware attacks.

Objective 2: Cyber risks are managed by those best placed to do so

How can Australia improve cyber security risk management across the economy and for critical infrastructure, in order to reduce the harm from cyber security incidents?

Issues

At its core, good cyber security means good risk management. This statement reflects an uncomfortable truth that cyber security threats cannot be eliminated – only identified and managed. In this way, cyber security is analogous with other important risk management issues in society, such as workplace health and safety, or natural disasters.

Many submissions to the 2020 Cyber Security Strategy suggested that Australia's approach to managing cyber security risk is immature. As part of its deliberations, the Panel reviewed Australia's legal framework for cyber security and the obligations placed on businesses to manage cyber security risk. This included a briefing from the Chair of the Australian Competition and Consumer Commission.

In many cases, the laws and standards of behaviour that apply in our physical world have not translated into, or been enforced in, the online world. When Australians purchase a digital product, it may be unclear to the consumer whether the provider is legally required to manage cyber security risks or to what standard. This can be either because of gaps in the law or because there is no precedent for current laws being used for cyber security. This means that end users may feel they have few avenues of recourse when an incident occurs and ultimately bear the costs.

Critical infrastructure providers face a different set of issues. Some sectors, particularly telecommunications and banking, have mature regulatory frameworks and actively engage with Government. Other critical assets such as data centres are unregulated. The powers that the Australian Government does have relating to critical infrastructure and cyber security are primarily reactive, focusing on information gathering or interventions of last resort. The current framework does not cover all industry sectors that many would consider to be of national significance. This leads to variable outcomes and in some areas does not fully meet community expectations of safety and security.

> *"Within a company cyber security is everyone's job. The board must do their part in ensuring the cyber risk is managed just as it does with all other key corporate risks"*
>
> **Robyn Denholm**
> Board Chair, Tesla

Our conclusions

In our opinion, the increased likelihood and consequences of cyber security incidents means there is a need for a national conversation about how cyber security risk is managed in the economy. We believe it is in the national interest for Government to work with industry to develop clear requirements for cyber risk management in a way that minimises regulatory burden and does not discourage innovation. Cyber security is a top-tier strategic issue and risk, and as such, the most senior leaders in both private and public sector organisations should have ultimate accountability for cyber security risk. For publicly listed companies, the board should be directly involved in understanding how cyber security risks are managed.

The Panel believes different requirements should be placed on a business depending on the level of risk the business engages with, the kind of product or service it is providing, and its revenue. Wherever possible, maturity frameworks should be used so that businesses improve their cyber security defences over an appropriate length of time. More digital infrastructure and businesses need to be considered 'critical' (for example data centres), compared to the current regulatory regime.

Government systems should not be treated differently to privately owned and operated critical infrastructure. Those responsible for defending public sector networks need to be held to the same standards as the private sector, including mandatory use of appropriate maturity frameworks (see Objective 4: Government is a cyber security exemplar).

Implementing these recommendations will take time. In the interim the Government should immediately encourage major vendors to sign-up to a voluntary security by design charter. Such a charter could focus on consistent implementation of proven and cost-effective cyber security controls, such as data encryption and multi-factor authentication. Negotiating a charter would signal Government's changed expectations in relation to cyber security and encourage industry to take appropriate steps in advance of any legislative change.

Our recommendations

In considering how Australia can improve cyber security risk management across the economy and for critical infrastructure, the 2020 Cyber Security Strategy should as an immediate priority:

8 Review the Australian Government's definition for critical infrastructure with a view to capturing all essential systems and functions in the public and private sectors and supply chains, including digital infrastructure such as data centres, that address all systems of national significance.

9 Introduce consistent, principles-based requirements to implement reasonable protection against cyber threats (where needed) for owners and operators of critical infrastructure (regardless of whether owned or operated by Government or private), with measurement based on a fit-for-purpose cyber maturity-based framework. In alignment with international best practice, this should leverage rather than duplicate existing sectoral regulations and minimise regulatory burden.

We further recommend that the 2020 Cyber Security Strategy should:

10 Review Australia's legislative environment for cyber security to ensure that suppliers of digital products and services have appropriate obligations to protect their customers.

11 Strongly encourage major vendors to sign-up to a voluntary 'secure by design' charter to leverage international best practice.

Objective 3: Australians practice safe behaviours at home and at work

How can Australia reduce human risk factors in cyber security?

Issues

By one estimate, 99 per cent of cyber security incidents require human error to succeed.[2] No matter how cyber secure products and services are made, individuals, families and businesses will always carry a level responsibility for their cyber security. Awareness raising and behaviour change initiatives are therefore necessary complements to technical cyber security protections to reduce Australians' exposure to online threats.

Knowledge of safe online behaviours isn't innate – it is through education that risks are appreciated and the steps to mitigate them are learned. During public consultation, many respondents called for more awareness raising and behaviour change initiatives to drive cultural change and encourage secure behaviours online.

A national-scale awareness raising campaign based on well-known public health campaigns such as 'Slip, Slop, Slap' was a particularly popular suggestion. The need to provide greater support to vulnerable groups, including families, small to medium enterprises and local councils was a common theme.

During its deliberations, the Panel received a briefing from the eSafety Commissioner and other senior officials on best practice approaches to behaviour change and awareness raising. There are currently a number of publicly funded campaigns led by different Government agencies, including the eSafety Commissioner (multiple initiatives), the Australian Cyber Security Centre (Stay Smart Online), the Australian Federal Police (Think U Know) and the Australian Competition and Consumer Commission (Scamwatch). Some stakeholders identified a need for Government to be more coordinated and targeted in its awareness raising efforts, which are sometimes perceived as confusing or overlapping as they target similar audiences.

The unique needs of small and medium enterprises (SMEs) were raised frequently during stakeholder consultation and directly with the Panel. SMEs are a critical part of the nation's economy, comprising 98 per cent of all Australian businesses. Most SMEs are taking simple steps to protect themselves however many are not — 39 per cent do not use multifactor authentication and 32 per cent do not make daily data backups.[3] SMEs engaged by the Panel took the strong view that the limited time and resources of small business owners are the key drivers of poor cyber security practices.

2 Proofpoint 2019, The Human Factor 2019 Report

3 Australian Signals Directorate 2019, Australian Cyber Security Centre Small Business Survey

> *"Government awareness raising programs need to be dramatically scaled up to reach more Australians. Existing programs also need to be better coordinated so that Australians aren't confused by multiple messages from different Government departments"*
>
> **Bob Mansfield AO**
> Chair, Vocus Group

Our conclusions

Awareness raising and behaviour change should be a priority for the 2020 Cyber Security Strategy, noting that human error is a factor in the vast majority of cyber security incidents. The primary limitation of existing efforts is scale. Government should consider additional investment to greatly extend or expand current campaigns, utilising existing programs and partnerships where possible with campaigns to be age and sector appropriate.

Noting the constrained fiscal environment, there are a number of innovative or cost-effective approaches that Government might consider. Government and industry both have an interest in raising awareness of cyber security threats, and the Panel believes that there is appetite for jointly funded and delivered campaigns. Another approach is to equip larger businesses to improve the cyber security awareness of small business customers and suppliers (similar to the campaigns already underway by some of Australia's largest companies). One industry example is Telstra's "five knows of cyber security" launched in 2015 to assist to manage the risk – know the value of your data, know who has access to your data, know where your data is, know who is protecting your data, and know how well your data is protected. Finally, Government should seek efficiencies of scale and improved coordination across existing public awareness campaigns in the areas of online safety, privacy and cyber security.

The Panel does not believe that traditional awareness raising campaigns will greatly assist SMEs. Instead, Government should pilot innovative programs that can address the needs of small business owners and account for the constrained time and resources of this target audience. One option would be to bundle cyber security advice as part of other business services, including from trusted advisers such as business groups or accountants. Another option would be to incentivise SMEs to upgrade legacy IT equipment, which would deliver both productivity and cyber security outcomes.

Our recommendations

In considering how Australia can reduce human risk factors in cyber security, the 2020 Cyber Security Strategy should as an immediate priority:

12 Unify all Government messaging on online safety and cyber security awareness raising, noting that existing campaigns run by different Government agencies share a common audience who do not distinguish between different online issues. Government should speak with one voice. Campaigns should be age and sector appropriate.

13 Increase assistance to small and medium businesses and the community through cyber security toolkits, trusted advice and practical assistance.

We further recommend that the 2020 Cyber Security Strategy should:

14 Partner with industry to increase the scale, reach and impact/effectiveness of cyber security awareness raising campaigns, including through co-design and co-funding where appropriate.

15. Incentivise large businesses to provide cyber security support to small and medium businesses in their supply chain and customer base.

Objective 4: Government is a cyber security exemplar

How can the Australian Government improve trust in the cyber security of its own systems and networks?

Issues

Cyber security goes to the very heart of the Government's digital transformation agenda. Without cyber security, public trust in Government services could be eroded and Australians won't benefit from the economic and social opportunities of the online world.

Recent incidents, such as the 2019 compromise of the Department of Parliamentary Services, show that Government is not immune to cyber security threats. Already, more than a third of citizens are unwilling to provide personal information to the Government because they don't trust it to keep data secure.[4] During public consultation, many stakeholders made it clear that the 2020 Cyber Security Strategy should not just ask the private sector to do more – Government itself needs to invest in the cyber security of the systems that underpin our democracy and are used by all Australians.

During its deliberations, the Panel received a detailed briefing from senior officials on how Government currently manages cyber security threats. It is clear that Government faces an extremely challenging task in lifting its own cyber security, with thousands of systems operated by hundreds of Government agencies both in Australia and overseas. This is true at the federal, state and local levels of government.

The Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) outline the steps that Australian Government agencies take to manage cyber security risks. The Information Security Manual includes four mandatory cyber security controls (the Top Four) that all agency heads must implement. While this is a mandatory requirement, there are variable cyber security outcomes because decision-makers implement this guidance differently, and have different attitudes to risk. The large number of government decision-makers involved in cyber security also creates barriers to coordination and in, some circumstances, diseconomies of scale.

The Panel understands that one of the biggest challenges facing Government is securing legacy systems that are vulnerable to cyber security threats. Legacy systems continue to be used because the cost of upgrading them is perceived to outweigh the cyber security risk. However, experience shows that legacy systems are frequently used by malicious actors as an initial entry point to a network. A similar tactic is being employed against smaller agencies that sometimes have lower levels of cyber security.

> *"All large organisations, including in Government, should adopt maturity frameworks to help them improve their cyber security over time. This recognises that improving cyber security takes time, focus and investment – it's not something that happens overnight"*
>
> **Chris Deeble AO CSC**
> CEO, Northrup Grumman Australia

4 *Government's digital agenda challenged by data distrust,* Canberra Times, 20 February 2020

Our conclusions

Government has a number of practical options for lifting the security of its systems and data, but there is no fast or easy one-size solution. Government should take a holistic approach to cyber security that includes personnel security, physical security and security of technology considerations. The Panel uses the term 'Enterprise Security Risk' to describe this holistic approach.

The Panel is of the view that Australian governments should be exemplars of enterprise security risk management for the private sector. To achieve this, strong executive sponsorship of security as a senior key business risk will be required. Recognising the importance of security through senior accountabilities will help set a cultural baseline for security practices, with an appropriately senior experienced Chief Security Officer necessary for credible leadership in managing enterprise security risk. The Panel would also welcome the ongoing transparency of government in publishing audits of cyber resilience practices across departments and stakeholder entities, with the findings of these reports highlighting opportunities for improvements and learning across all sectors.

The Panel is of the opinion that Government systems should be treated in the same way as critical infrastructure owners in the private sector. There should be mechanisms that hold decision-makers to account when agreed cyber security controls are not implemented. While the Panel notes that agency heads face long-term resourcing challenges, without stronger incentives Government agencies are unlikely to prioritise their funding of cyber security risk management over meeting businesses outcomes (this can also occur in the private sector). Over time, Government should investigate alternative funding models.

Another priority for Government should be addressing risks to small agencies that lack the resources to protect themselves from sophisticated threats and decommissioning vulnerable legacy systems. Larger agencies should be given responsibility for IT service delivery where this approach can reduce risk to small agencies. These recommendations are consistent with the recent Thodey Review of the Australian Public Service, which recommended improving the 'funding, structure and management of digital functions across the Australian Public Service'. Consideration should also be given to consistency and uniformity of IT infrastructure and therefore cyber security in the local government arena by having state governments and territories providing local governments with their IT infrastructure.

Digital change across the Australian Public Service will require a concerted, long-term and centrally-coordinated effort to overcome inertia and the inevitable complexity inherent in all technology projects. Digital reform should be approached as a large scale change management process, requiring sustained engagement by ministers and agency heads across all portfolios.

Government should also consider centralisation or better coordination of cyber security risk management across the Australian Public Service. Priority should be given to coordinating procurement to achieve cost savings and share cyber security capabilities across agencies. Cyber security clauses in Government contracts should be standardised where appropriate. These changes will allow Government to realise economies of scale.

The Panel recognises that the necessary rigour of Government procurement processes may inhibit best practice suppliers from engaging. It is also important to highlight that over reliance on single vendors, technologies or solutions may contribute to vendor lock-in or generate a concentration risk.

While agency heads are ultimately responsible for cyber security outcomes, they should continue to receive strong support from the Australian Cyber Security Centre (ACSC) through its rolling program of cyber security assistance. The Panel does not support the ACSC having a role in auditing government agencies, noting this would conflict with their role of providing support and assistance.

Our recommendations

In considering how Australia can improve trust in the cyber security of its own systems and networks, the 2020 Cyber Security Strategy should as an immediate priority:

16 Make all Australian governments exemplars of enterprise security risk management, including cyber security, physical security and personnel security.

17 Require Government agencies providing essential services to meet the same cyber security standards as privately owned critical infrastructure, with increased accountability and oversight.

18 Prioritise the decommissioning or hardening of vulnerable legacy systems as part of an accelerated shift towards secure cloud based services.

We further recommend that the 2020 Cyber Security Strategy should:

19 Better coordinate digital procurement decisions across Government, with a view to negotiating best practice outcomes and where appropriate cost savings with common vendors.

20 Leverage Government procurement processes to improve cyber security through purchasing products and services with higher standards.

21 Require larger, more capable Government departments to provide cyber security services to smaller agencies on a basis that is uniform, consistent and risk based.

22 Fund the Australian Cyber Security Centre (ACSC) to continue its rolling program of cyber security improvements (but not audits) for other Australian Government agencies. Given the ACSC essentially provides a second line of defence role in risk management terminology, audit should be undertaken by a separate agency.

Objective 5: Trusted goods, services and supply chains

How can Australia encourage the development of a digital technology market where security is built-in across the supply chain?

Issues

Australian families and businesses are not, in most cases, cyber security experts. Most buyers, whether they are individuals or businesses, find it difficult to know if they can trust digital products and services to be secure because they don't know what they should be looking for.

There is an opportunity to encourage, or incentivise, industry to deliver products and services with good cyber security. Manufacturers that do build security into products may not be rewarded if they compete on security grounds. There are few consequences for those that do not meet acceptable security standards (as discussed under Objective 2: Cyber security risks are owned by those best placed to manage them). The slow uptake of controls that are cheap and easy to implement, such as unique passwords on consumer devices and multi-factor authentication, illustrates that technology markets are immature in their approach to cyber security.

There is very strong support in the community for Government to increase consumer trust in digital products by promoting 'security by design'. This means that, wherever practical, digital technologies should come with cyber security built-in to minimise the steps the consumer has to take to protect themselves. Initiatives used successfully in the broader economy to provide assurance to consumers, like product labelling and standards, are missing in cyber security. Insurance, a key tool for managing business risks, including triaging

and helping the victims of cybercrime, is at a lower level of maturity and uptake in cyber security compared to other areas.

Another challenge is the desire of some nation states to dominate critical and emerging technology markets for strategic advantage. The opaque and complex nature of supply chains makes it difficult to create assurance that a compromise has not occurred someone within the chain. Each component part introduces a potential vulnerability and could be compromised. For example, if a compromised network interface card is integrated into various products, each product with that card becomes vulnerable. Many businesses want to increase transparency in their supply chains and are seeking additional guidance from Government about how to manage these risks.

> *"It is difficult to overstate the importance of securing Australia's digital supply chains. Government and industry need to work more closely together, and with their international peers, on standards, research and development, transparency, and assurance measures. It would be a costly mistake to ignore this problem"*
>
> **Andy Penn**
> CEO, Telstra

Our conclusions

Government can take a number of actions to empower businesses and consumers to choose digital products and services that are 'secure by design'. A first priority is to work with industry to accelerate the adoption of cyber security standards in Australia. Noting that standards are only valuable if adopted widely, Government should use its convening power to build industry consensus around what standards should be used in Australia. As a complementary activity, the Government should establish either an accreditation or product labelling scheme to increase the transparency of cyber security protections at the point of sale. It may also be appropriate for Government to implement a certification scheme for digital supply chain participants.

The Panel believes that a mature cyber security insurance market has significant potential to improve Australia's cyber security resilience and influence the cyber security behaviours of policy holders. These are objectives that should be strongly supported by Government without direct intervention. Instead, Government should support development of the cyber security insurance market by coordinating access to reliable actuarial data and working with industry on evidence-based approaches to behavioural nudges for policy holders.

The Australian Government should work with its international partners to build trust and transparency into the supply chains for critical and emerging technologies. A first step is to develop a formal program for identifying emerging technologies that could introduce vulnerabilities into technology supply chains. Government should work closely with industry and likeminded countries on this activity. Through AustCyber, Government should continue to encourage small and medium businesses to take advantage of economic opportunities to act as a trusted cyber security supplier.

Further, the Australian Government should increase investment and encourage industry investment in sovereign cyber security research and development that supports both economic and national security outcomes. A strong

sovereign research and development capability is critical to Australia's ability to access trusted sources of technology and influence global decision-making bodies. Investment should prioritise commercialisation and basic sciences – two areas where Australia is lagging behind international best practice. The Government should also take a more active role in international forums to ensure our national interests are adequately incorporated into future standards.

Our recommendations

In considering how the Australia can encourage the development of a digital technology market where security is built-in across the supply chain, the 2020 Cyber Security Strategy should as an immediate priority:

23 Increase investment in cyber security research and development, including basic sciences, and coordinate state and territory-led research and development at the national level. This will enable Government to maximise economic opportunities and drive national security outcomes.

24 Work with industry to increase Australia's role in shaping international cyber security standards.

25 Work with industry and likeminded nations to encourage diversity, transparency and competition in digital supply chains.

We further recommend that the 2020 Cyber Security Strategy should:

26 Develop a program to identify and assess emerging threats and emerging technologies that could introduce new vulnerabilities leveraging Australia's global leadership in policy development related to cyber risks. The CSIRO and Defence Science and Technology are two existing national agencies that could be leveraged to support the development of this program.

27 Obtain industry consensus around what cyber security standards should be used in Australia and accelerate the adoption of these standards to ensure digital products and services are 'secure by design'.

28 Require increased recognition and adoption of specific cyber security standards in Australia.

29 Implement a dynamic accreditation or mandatory cyber security labelling scheme so that consumers can make informed choices about their own cyber security (recognising that accreditations and product labelling will need to take account of changes in technology).

30 Work with the emerging cyber insurance industry to improve access to reliable actuarial data and develop best practice approaches to nudging the cyber security hygiene of policy holders.

31 Build transparency into critical and emerging technology supply chains to enable consumers to trust the cyber security of their devices.

32 Consider mandatory requirements or certification of supply chains for software and hardware supporting critical infrastructure.

Objective 6: Comprehensive situational awareness enables action

How can Government and industry improve shared situational awareness and act in real-time to prevent threats from reaching end users?

Issues

Situational awareness is essential for strong cyber security. Being able to identify threats before or while they are occurring allows Government and industry to take action to prevent or minimise harm.

During its deliberations, the Panel received a classified briefing from the Australian Signals Directorate about its capabilities to detect and respond to cyber security threats against critical infrastructure. Sophisticated actors go to great efforts to hide their cyber activities, which presents an ongoing challenge to Australia's national security agencies. There are also technical and legislative limitations on what these agencies can do once they are aware of a serious threat.

During consultation, many stakeholders supported the increased use of threat blocking technology (for example, blocking known malicious websites). The advantage of this approach is that it does not require any user education to be effective. Some types of threat blocking are already used widely. The Panel acknowledges Telstra's "cleaner pipes" initiative announced in May 2020 which involves significantly upscaling Telstra's Domain Name System (DNS) filtering, where millions of malware communications are being proactively and automatically blocked every week as they try to cross Telstra's infrastructure. Many stakeholders pointed to the United Kingdom's Active Cyber Defence program as a best practice model for Australia to emulate. Support for blocking threats at scale was the highest among those on the front lines of the battle against cybercrime – particularly financial institutions.

The Panel noted consistent feedback from stakeholders about the need to improve Australia's situational awareness through improved threat information sharing between industry and Government. The primary concern was a perceived lack of real-time threat information sharing from the Australian Cyber Security Centre to industry. Many industry participants also sought legislative certainty (so called 'safe harbours') about the cyber security information they can share with other businesses.

> *"Situational awareness is an essential element of strong cyber security. In a modern economy like Australia businesses and Government both have threat intelligence that needs to be shared routinely with each other and in real-time"*
>
> **Kirstjen Nielsen**
> Former U.S Secretary of Homeland Security

Our conclusions

Improving situational awareness of cyber security threats to organisations of all kinds should be a national priority.

There is clear appetite from industry for real-time sharing of threat information. The Panel was surprised to learn that technical limitations currently prevent the Australian Cyber Security Centre from meeting these requests. These limitations are surmountable and should be addressed as a priority. The Panel also supports greater legal clarity on what information businesses can share with each other for the purpose of preventing or responding to a cyber security incident and establishment of "safe harbour" coverage for businesses that work with ACSC.

In terms of privately owned critical infrastructure, the Panel recognises that network owners are usually best placed to respond to threats against their own networks. However, there are unique capabilities that Government can contribute, particularly in response to state sponsored threats. How Government goes about improving its situational awareness is critically important. Strong partnerships with industry, robust oversight mechanisms and clear communication with the community should be foundational principles for action. These same principles should apply if Government determines that expanded legislative powers are required in unregulated critical sectors to gather threat information or respond to threats once identified.

The Panel strongly supports the increased use of threat blocking for low-sophistication threats. The Government should lend its direct support to any industry-led threat blocking initiatives. Government's role should include providing funding support and legislative certainty where required, particularly over the long-term so that threat blocking capabilities can be continuously improved. This should lead to a long-term continuous improvement to both the public and private sector threat blocking capabilities.

Our recommendations

In considering how the Government and industry can improve the timeliness and quality of threat information sharing to better anticipate and respond to threats, the 2020 Cyber Security Strategy should as an immediate priority:

33 Establish automated, real-time and bi-directional threat sharing mechanisms between Government and industry, beginning with critical infrastructure sectors.

We further recommend that the 2020 Cyber Security Strategy should:

34 Empower industry to automatically block a greater proportion of known cyber security threats in real-time, including by providing legislative certainty.

35 Consider the development of 'safe harbour' legislative provisions that give industry certainty about the information it can voluntarily share with other organisations to prevent or respond to cyber security threats.

36 Resume the publication of annual reports on the state of cyber security threats to Australia.

Objective 7: Effective response options and victim support

How can Government and industry create and sustain a high level of preparedness for incidents, and improve support to victims?

Issues

Malicious cyber activity is hitting Australians hard. The tactics and techniques used by malicious cyber actors are evolving so quickly that individuals, businesses and critical infrastructure owners and operators in Australia are not able to protect themselves and their assets against every cyber security threat. Statistics confirm this – the Australian Cyber Security Centre received 26,500 reports of cybercrime in the second half of 2019 alone, while a Frost & Sullivan study commissioned by Microsoft found that cyber security incidents cost Australian businesses up to $29 billion in direct costs each year. Although Government has various restorative mechanisms in place, they are not adequately calibrated to respond to these rising figures.

Different approaches to cyber security resilience are required at the personal, commercial and national levels to effectively mitigate damage and restore key systems.

In relation to critical infrastructure, the Panel received advice from the Department of Home Affairs that current laws may not allow Government to respond quickly enough if a major cyber incident affected multiple critical infrastructure systems at once and where some providers are not regulated. The current framework does not cover all industry sectors that many would consider to be of national significance. This leads to variable outcomes and is some areas does not fully meet community expectations of safety and security.

The Panel also noted stakeholders' views that Government should collaborate more closely with critical infrastructure to increase preparedness for major, cross-sectoral cyber incidents, for example by conducting cyber security exercises in partnership with the private sector. Stakeholders also proposed updating Australia's national framework for managing and practicing responses to significant cyber incidents – the national Cyber Incident Management Arrangements – to incorporate the role of industry.

In relation to individual incidents, the Panel found constrained funding for charities offering counselling to victims of cybercrime particularly concerning. We heard that the growth in the number of cybercrime victims has outpaced the level of support available, putting enormous pressure on community organisations such as IDCARE, Australia and New Zealand's national identity and cyber support community service. IDCARE's written submission to the public consultation highlighted that demand for its services is growing at an annual rate of 57 per cent.

> *"Most cybercrime has a human victim. We need to do a better job of providing personalised support to help Australians get back on their feet after a traumatic experience like fraud or identity theft"*
>
> **Darren Kane**
> Chief Security Officer, NBN Co

Our conclusions

The 2020 Cyber Security Strategy needs to ensure that Australia is resilient in the face of cyber incidents and impacts to Australians are minimised. If a major cyber-attack were to target a critical infrastructure system – or several systems at once – the ramifications for our society and economy could be very high.

Understanding the connections and dependencies and interdependencies between critical systems is not an easy task, particularly when supply chains are also considered. There are few formalised mechanisms for critical infrastructure owners to share highly detailed information about dependencies and interdependencies, and as a result neither Government nor the private sector has a consistent and adequate understanding of cyber security dependencies and interdependencies. A sustained effort from both Government and industry is required to identify and manage these critical dependencies and interdependencies. In doing so, the Panel recommends that Government and industry leverage the modelling capability of the Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience www.tisn.gov.au.

Government should also further prepare for low probability, high consequence attacks by working with the private sector to identify the very limited circumstances when it would be appropriate and necessary for Government to take an active role in helping to restore critical systems.

The Panel concurs with stakeholder feedback that Government and law enforcement should work with industry to conduct an expanded national program of regular, cross-sectoral cyber exercises. These exercises must be underpinned by modelling, simulation and vulnerability assessments (in testing the system under controlled conditions). This is a proven model internationally and will assist both Government and industry to improve their readiness. Government should also update the current Government incident response 'playbook' (known as the Cyber Incident Management Arrangements) to formally recognise the role of the private sector in responding to incidents.

In relation to individuals and small and medium businesses, the Panel recommends that the 2020 Cyber Security Strategy provide increased support to world class support organisations to facilitate these organisations' ongoing growth and enable more cybercrime victims to access much-needed specialist services. The Panel is particularly conscious of the thin profit margins that many operate on, and their reduced ability to respond to a cyber security incident. In regional areas many communities have an increased reliance on SMEs, which makes their speedy recovery from cyber security incidents even more important.

Our recommendations

In considering how Government and industry can create and sustain a high level of preparedness for incidents and improve support to victims, the 2020 Cyber Security Strategy should as an immediate priority:

37 Map in partnership with industry, the resilience of critical infrastructure networks, with a view to increasing maturity levels over time.

38 Identify and assess in partnership with industry interdependencies, single points of failure and consolidation risk to enable better understanding of cyber risk.

39 Work with industry to agree a unique circumstances in relation to critical infrastructure and systems of national significance when it would be appropriate for Government to directly assist Australian businesses during a cyber security emergency, and define suitable oversight and thresholds for action.

40 Provide additional funding to not-for-profit organisations that support victims of cybercrime and communicate their role and existence to the community.

We further recommend that the 2020 Cyber Security Strategy should:

41 Hold a large scale and cross-sectoral cyber security incident response exercise at least every two years to improve national coordination and incident response readiness of interdependent critical infrastructure providers and government agencies. Exercises should include links to international activities where appropriate.

42 Include industry in Australia's formal incident response plans by amending the national Cyber Incident Management Arrangements.

Enabler 1: The Australian Signals Directorate's Joint Cyber Security Centres

How can Government and industry mature collaboration through the Joint Cyber Security Centre Program?

Issues

The Joint Cyber Security Centre (JCSC) Program was a key initiative of the 2016 Cyber Security Strategy, designed to build practical cyber security partnerships between business, academia and government agencies. There was almost unanimous feedback from industry and academia that the Program is highly valuable and should continue.

The Program currently has more than 700 organisations as members and offices located in most of Australia's capital cities (the Brisbane and Melbourne offices engage remotely and in-person with stakeholders in Darwin and Hobart respectively). Each Centre has a sectoral specialisation that guides their work (for example, Brisbane is the lead for the energy sector). Telstra and NBN Co both participate in the JCSC Program.

Typical JCSC activities include incident response coordination, threat information sharing, training, program delivery, stakeholder consultation, and locally guided collaboration opportunities and projects. Feedback from industry highlighted the pivotal role JCSCs play in coordinating responses to major incidents and facilitating practical collaboration on cyber security between organisations who would not otherwise engage with each other.

While there was widespread support for the JCSCs, there was consistent feedback that this initiative has not yet reached its full potential. Industry is calling for the JCSCs to have greater resourcing and a stronger role in delivering practical cyber security services. Similarly, academia wants the JCSCs to play a stronger role in guiding practical research.

Stakeholder feedback also pointed to confusion about the JCSCs' practical deliverables. There are perceptions that a focus on establishing physical facilities and running events has come at the expense of tangible cyber security outcomes. After receiving a detailed briefing from the Australian Signals Directorate, it is clear that the JCSCs face practical challenges, particularly a reliance on interim governance arrangements and uncertainty about precise deliverables.

> *"The Joint Cyber Security Centres are an incredibly valuable program. I have complete confidence they will only grow and improve in the future with further investment and a national governance framework"*
>
> **Andy Penn**
> CEO, Telstra

Our conclusions

The Panel believes that the JCSCs are a highly valuable national asset and should form a key delivery mechanism for the initiatives under the 2020 Cyber Security Strategy. The JCSCs should continue to play a role in building strong cyber security partnerships between businesses, the research community, and Government. However, the Panel agrees with other stakeholders that the JCSCs are yet to realise their full potential.

The Government should consider changes to the JCSC operating model to better deliver on the original intent of operational and strategic level cooperation with industry. The Panel notes that interim industry steering committees are still operating three years after the Program began, which is contributing to uncertainty in strategic direction. As a first priority, the Government should finalise governance arrangements, maintaining a role for industry leadership. An overarching national board should be implemented to help bring national consistency to the Program.

The Panel cautions against the Program trying to be 'all things to all people'. Priority should be given to improving operational capability and delivering services. This will provide a stronger basis for practical collaboration with industry and will reduce the current reliance on collaboration through events. The JCSCs may need additional resourcing to achieve their mission.

Our recommendations

Recognising the JCSCs are the local offices of the Australian Cyber Security Centre, the 2020 Cyber Security Strategy should as an immediate priority:

43 Establish a national board chaired by ASD (with industry co-chair) and including industry representation to strengthen the strategic leadership of the Joint Cyber Security Centres, underpinned by a charter outlining the JCSCs' scope and deliverables.

44 Fund ASD to provide enhanced technical and consulting cyber services to industry through the JCSC Program, including a greater focus on information sharing.

We further recommend that the 2020 Cyber Security Strategy should:

45 Create a staff exchange program between the ACSC, academia and industry to enable cross-sectoral collaboration and information sharing. The CSIRO and Defence Science and Technology could be leveraged to support the engagement between academia and industry.

46 Dedicate additional JCSC resources to engage with local governments.

Enabler 2: Cyber security skills

How can Government, industry and academia improve risk postures by strengthening the pipeline of skilled cyber security professionals?

Issues

There is evidence from some submissions and other data sources that a shortage of appropriately skilled cyber security professionals is having a negative impact on Australia's ability to prevent and respond to cyber security incidents. This problem was one of the top five issues raised by industry, academia and the community during public consultation on the 2020 Strategy.

Most businesses believe that Australia's education and training system is not meeting their requirements. There are widespread views that most graduates lack the real-world experience needed to be job-ready, and that curricula are not keeping pace with technological change and changing adversary tactics.

Education and training institutions often face barriers in teaching cyber security. Some institutions feel there is poor communication from industry about skill requirements. Many tertiary and vocational institutions seek to prepare their graduates for the workforce by including work experience in their courses, but in some cases there are difficulties in finding industry partners. It is also difficult for academia to attract and retain educators with industry experience. Some stakeholders submitted that these problems are compounded by the absence of a shared definition for 'cyber security professional' and a lack of reliable data on the size of the skills shortage in Australia.

> *"Skilled employees are an essential part of strong cyber security. We need to think about how Australia manages its finite pool of cyber security experts across the whole economy. It's not just a matter of training more graduates"*
>
> **Chris Deeble AO CSC**
> CEO, Northrup Grumman Australia

Our conclusions

Industry and academia need to work more closely together to attract, train and retain cyber security talent in Australia. This should be coordinated at the national level.

The Panel welcomes Government's election commitment for a $50 million Cyber Security National Workforce Growth Program, which will be implemented as part of the 2020 Cyber Security Strategy. The Program will include a range of activities such as scholarships and development of specialist cyber security courses.

The Cyber Security National Workforce Growth Program should be supported by nationally coordinated policy changes to ensure the education and training system is able to keep pace with technological change. A first priority is creating stronger feedback mechanisms between industry and academia, so that everyone understands what skills are required in the workforce, even as technology and adversary tactics change rapidly.

A shared definition for the different roles that make up the cyber security profession in Australia is a basic but essential first step on this journey. Once this has been achieved Government should focus on facilitating national recognition of the skills and experience of cyber security professionals across the full spectrum of cyber security roles. Practicing requirements, such as continuing education and standards of ethical behaviour, should be considered in line with established professions such as accounting and law.

Australia should also make greater use of voluntary professional accreditation for university cyber security courses, so that students and employers have confidence that they meet the current industry needs. We believe that cyber security should be included in university-level technical courses outside of the cyber security profession, particularly related technical fields like engineering and data science. Finally, we agree with many others in the community that cyber security education should begin early, including in primary school, as part of a broader approach to Science Technology Education and Maths (STEM) education.

All future policy initiatives should be underpinned by survey data to assist policy makers, academia and other interested stakeholders to understand the precise quantum of the cyber security skills shortage and the impact of the 2020 Cyber Security Strategy.

Our recommendations

In considering how Government, industry and academia improve risk postures by strengthening the pipeline of skilled cyber security professionals, the 2020 Cyber Security Strategy should:

47 Position the Australian Government to take a national leadership role in addressing Australia's cyber security skills shortage.

48 Work with professional bodies and academia to include cyber security education in adjunct technical fields such as engineering and data science and extend cyber skills training to company directors.

49 Consider creating an internationally aligned accreditation scheme to recognise the skills, experience and qualifications of cyber security professionals in both technical and management roles. This should including mapping the equivalency of existing qualifications.

50 Adopt a national framework that defines the roles that make up the cyber security profession. Use this framework to develop a national workforce planning program for the cyber security profession.

51 Consider additional incentives to attract and retain Government cyber security specialists.

52 Strengthen voluntary professional accreditation of university cyber security courses, to provide greater assurance to students and employers that courses are meeting contemporary industry demands.

53 Develop targeted cyber security programs in primary and high school to inspire young people to take up a career in cyber security, and build foundational skills in science, maths, engineering and technology.

54 Undertake a regular survey across Government and business to better understand the size of cyber security skills shortage in Australia and evaluate new programs under the 2020 Cyber Security Strategy.

Enabler 3: Intelligence and Assessment

The Panel recognises the importance of intelligence-led efforts to combat malicious cyber activity and acknowledges that this is primarily a matter for Government. The Panel is of the view that successful implementation of the recommendations above relating to Objective 1 (Clear consequences for targeting Australia and Australians), Objective 6 (Comprehensive situational awareness enables action) and Enabler 1 (The Australian Signals Directorate's Joint Cyber Security Centres) will support Government to enhance the delivery of this enabler.

The Panel encourages the Government to be open and transparent about its knowledge of the threat environment wherever possible, including by declassifying information when appropriate, increasing proactive cyber threat briefings to security cleared industry personnel with a need to know, and sponsoring greater numbers of industry representatives to obtain security clearances.

Enabler 4: Governance

How should Government manage implementation of the Strategy, including oversight arrangements, ongoing industry consultation and reporting mechanisms?

Issues

During consultation stakeholders made it clear that the only good strategy is one that is implemented effectively. Some stakeholders viewed implementation of the 2016 Cyber Security Strategy as being limited by regular changes in governance arrangements, confusion about the roles of different government departments and inconsistent public communication.

> *"One essential part of successful Strategy implementation is communication. Communicate, communicate, communicate"*
>
> **Bob Mansfield AO**
> Chair, Vocus Group

Our conclusions

Transparent governance and oversight mechanisms will address many of the concerns raised about implementation of the 2016 Strategy.

An external advisory panel should be established to advise Government on cyber security issues, including implementation of the 2020 Strategy. This would improve public communication during implementation and provide a forum for industry to raise any concerns directly with senior officials in a timely manner. The panel should have broad representation from across business, academia and the community. The panel would ensure accountability by providing regular reports to the Minister for Home Affairs and to the broader public. A formal report should be published on an annual basis.

The panel should not be a substitute for ongoing industry consultation.

State and territory governments should be closely involved in implementation of the Strategy. It would be appropriate for state and territories to be represented on the public service committee responsible for implementing the Strategy.

Our recommendations

In considering how Government should manage implementation of the Strategy, including oversight arrangements, ongoing industry consultation and reporting mechanisms, the 2020 Cyber Security Strategy should as an immediate priority:

55 Include state and territory Governments in development, implementation and monitoring of all relevant initiatives under the 2020 Cyber Security Strategy.

We further recommend that the 2020 Cyber Security Strategy should:

56 Appoint an industry advisory panel to advise the Government on cyber security on an ongoing basis, including on the implementation of the 2020 Cyber Security Strategy. The panel should work with the accountable Government agency or department responsible for implementing the Strategy, while reporting to the Minister for Home Affairs.

57 Task the industry advisory panel to publish an annual progress report on implementation of the 2020 Cyber Security Strategy and emerging cyber security threats and priorities for Australia from an industry perspective.

Enabler 5: Evidence and Evaluation

What best practice approaches to evidence collection and evaluation can inform implementation of the Strategy and future policy making?

Issues

The effectiveness of all Government policies should be measurable. This is in line with clear direction from the Prime Minister to the Australian Public Service.

Evaluation of cyber security initiatives is challenging because it is difficult to prove that cyber security incidents were prevented.

Specialist skills are required for data collection, analysis and evaluation (sometimes generalist public servants are expected to perform these duties). A number of international and domestic public sector organisations have specialist resources dedicated to evidence and evaluation. For example, the UK National Cyber Security Centre has an evidence unit that contributes to public evaluation of its cyber security strategy.

Measurement of cyber security metrics needs to be based on a maturity model, as cyber security is not a binary state where an organisation is either secure or not.

Currently, there is a lack of contemporary, long-term, and statistically representative data on the impact of cyber security incidents in Australia. As a result, decision-makers within Government often rely on intelligence assessments, incomplete data and case studies.

> *"To improve cyber security maturity both Government and industry need to know what they're measuring. Too often good metrics and data collection are neglected during implementation"*
>
> **Chris Deeble AO CSC**
> CEO, Northrup Grumman Australia

Our conclusions

Performance metrics should be developed for all initiatives under the 2020 Strategy. Improved data collection and analysis is necessary to develop meaningful metrics and respond to stakeholder feedback that evaluation needs to focus more heavily on outcomes.

A best practice approach to evaluation would also include the semi-independent evaluation of strategy initiatives by external contractors, with a focus on constructive feedback. Evaluations, as well as regular updates on strategy implementation, should be made publicly available to provide increased transparency in implementation of the 2020 Strategy.

Our recommendations

In considering the best practice approaches to evidence collection and evaluation that can inform implementation of the Strategy and future policy making, the 2020 Cyber Security Strategy should:

58 Adopt a maturity model approach to evidence and evaluation.

59 Invest in improved data collection, research and analysis to underpin evaluation of performance against the metrics of the 2020 Cyber Security Strategy. This should include periodic surveys of the cyber security maturity of public and private sector organisations.

60 Publish regular updates on implementation of the 2020 Cyber Security Strategy and periodically review and refresh the Strategy every 2 or 4 years.

Appendix 1:
Industry Advisory Panel Terms of Reference

Purpose

The Minister for Home Affairs has established a Cyber Security Strategy Industry Advisory Panel to provide strategic advice to support the development of Australia's 2020 Cyber Security Strategy.

Term

The Panel will continue during the development of the next Cyber Security Strategy. After the release of the Cyber Security Strategy, the role of the Panel and its membership may be reviewed. The Panel may need to continue to advise on implementation of the Strategy.

Roles and Responsibilities

The Panel is responsible for providing strategic advice to the Minister for Home Affairs and the Department of Home Affairs on the development of the 2020 Cyber Security Strategy. The role of the Panel is purely advisory and members of the Panel are not acting on behalf of the Department or making any decisions.

The 2020 Cyber Security Strategy will seek to:

- protect and secure nationally significant infrastructure, systems and data;
- ensure cyber-risk is managed appropriately in the economy and community;
- improve assistance and support to individuals, families and small businesses;
- build a mature and trusted domestic market for secure technologies, products, services and professionals;
- create new ways for businesses and individuals to prosper in the digital age; and
- strengthen our cyber security capability.

The Panel is expected to provide advice on:

- best practices in cyber security and related fields;
- emerging cyber security trends and threats;
- key strategic priorities for the 2020 Cyber Security Strategy;
- significant obstacles and barriers for the delivery of the 2020 Cyber Security Strategy; and
- the effect of proposed initiatives on different elements of the economy, both domestic and international.

Members of the Panel will:

- provide their expertise to contribute to the development of Australia's 2020 Cyber Security Strategy;
- provide feedback and advice in a timely manner;
- share knowledge and experience across all Panel members in a trusted environment;
- maintain appropriate discretion and confidentiality with respect to the Panel's business;
- avoid making public comments about the matters considered by the Panel unless they make clear that they are expressing personal views only; and
- disclose any relevant interest at any meetings of the Panel as soon as possible after the relevant facts have come to the member's knowledge.

Meetings

The Panel will be chaired by Mr Andrew Penn with support from the Department of Home Affairs.

The Department of Home Affairs will provide a secretariat function. This includes:

- providing direction during discussions of specific topics;
- preparing agendas and supporting papers;
- preparing and disseminating meeting notes and information;
- following up on actions; and
- keeping members informed of developments and activities between meetings.

Scheduled meetings will be held on an approximate monthly basis. Formal briefings to the Minister for Home Affairs will occur at key points in the development of the 2020 Strategy.

The Panel may meet in person or via video teleconference. Travel expenses agreed in advance with the Secretariat will be covered by the Department of Home Affairs.

Panel members will be unremunerated.

Appendix 2:
About the Panel

Mr Andrew Penn

Mr Penn is Chief Executive Officer and Managing Director at Telstra, Australia's largest telecommunications company. He has had an extensive career spanning 40 years to CFO and CEO level and across three industries - telecommunications, financial services and shipping. He is a board director of the GSMA representing the telecommunications industry globally and a supporter of numerous charitable and social causes.

Ms Kirstjen Nielsen

Ms Nielsen served as the U.S. Secretary of Homeland Security from 2017–2019 and was responsible for all operational, policy, and legal matters, including counter-terrorism, cyber security, and border security. Prior to this, Ms Nielsen served as White House Deputy Chief of Staff and Chief of Staff to then-Secretary of Homeland Security, and held a range of public and private advisory roles focused on national security, strategy, preparedness and critical infrastructure.

Mr Robert Mansfield AO

Mr Mansfield is Chair of Vocus Group, a telecommunications infrastructure provider. He has held several CEO positions, including at Optus Telecommunications, and has filled a number of specialist roles for the Australian Government, including as Strategic Investment Coordinator within the Prime Minister's Office. In 2000, Mr Mansfield was appointed as an Officer of the Order of Australia for his contribution to Australian business and economic development and to the telecommunications industry.

Ms Robyn Denholm

Ms Denholm was appointed Board Chair of Tesla in 2018 and has served as a director since 2014. She was previously Chief Operations Officer at Telstra and held a number of senior positions at Juniper Networks, a networking equipment manufacturer. Ms Denholm's extensive corporate experience also includes Sun Microsystems, Toyota Motor Corporation, Arthur Andersen and Company (an accounting firm) and ABB Ltd (an industrial technology company).

Mr Chris Deeble AO CSC

Mr Deeble is Chief Executive of Northrop Grumman Australia, a provider of cyber security solutions to Australia's Defence Force. Prior to this he worked for Airservices Australia and served in the Australian Defence Force. In 2007 he was awarded the Conspicuous Service Cross. In 2016 he was appointed as an Officer of the Order of Australia for distinguished service to the Australian Defence Force.

Mr Darren Kane

Mr Kane has been the Chief Security Officer (CSO) at NBN Co since March 2015. As CSO, Mr Kane has sole accountability for enterprise-wide management of all security risks in Australia's biggest infrastructure project. His career has included 13 years with the Australian Federal Police and 6.5 years with the Australian Securities and Investments Commission. Mr Kane moved to Telstra in 2004 where he completed 11 years in varied management roles culminating in 4.5 years as Director, Corporate Security and Investigations.

Appendix 3:
Problem Statements

Issue	Problem Statement
Cyber risk management	How can Australia improve cyber security risk management across the economy and for critical infrastructure, in order to reduce the harm from cyber security incidents?
Hardening Government systems	How can the Australian Government improve trust in the cyber security of its own systems and networks?
Enhanced situational awareness and threat blocking	How can Government and industry improve shared situational awareness and act in real-time to prevent threats from reaching end users?
Trusted goods, services and supply chains	How can Australia encourage the development of a digital technology market where security is built-in across the supply chain?
Threat information sharing	How can government and industry improve the timeliness and quality of threat information sharing to better anticipate and respond to threats?
Behaviour change / awareness raising	How can Australia reduce human risk factors in cyber security?
Joint Cyber Security Centres	How can Government and industry mature collaboration through the Joint Cyber Security Centre Program?
Malicious actors held to account	How can Australia increase the consequences of malicious cyber activity for nation states and cyber criminals?
Incident response	How can Government and industry create and sustain a high level of preparedness for incidents, and improve support to victims?
Cyber security skills	How can Government, industry and academia improve risk postures by strengthening the pipeline of skilled cyber security professionals?
Evidence and evaluation	What best practice approaches to evidence collection and evaluation can inform implementation of the Strategy and future policy making?
Governance and implementation	How should Government manage implementation of the Strategy, including oversight arrangements, ongoing industry consultation and reporting mechanisms?