KPMG

2023-2030 Australian Cyber Security Strategy Discussion Paper

KPMG submission

KPMG Australia, May 2023
KPMG.com.au

Contents

Executive summary

As a leading professional services firm, KPMG Australia (KPMG) is committed to meeting the requirements of all our stakeholders – not only the organisations we audit and advise, but also employees, governments, regulators – and the wider community. We strive to contribute in a positive way to the debate that is shaping the Australian economy and we welcome the opportunity to provide a submission to the *2023-2030 Australian Cyber Security Strategy Discussion Paper* (the discussion paper) building on our September 2021 submission in response to the *strengthening Australia's cyber security regulations and incentives* discussion paper.[1]

The Australian cyber landscape has been particularly dynamic since our last submission and the release of the former government's Cyber Security Strategy in 2020. But still, many of the priority topics, from skills and sovereign industry through to the legislative environment and critical infrastructure protection, remain constant.

KPMG welcomes the Government's ambition and sees it as a national imperative to work towards Australia being the most cyber secure nation in the world by 2030. This Strategy will need to catalyse activity across the nation towards this objective, strengthening Australia's collective ability to prevent, deter, detect, respond to and recover from cyber incidents, as well as enabling greater commercial and market opportunities for our sovereign cyber industry. But to be successful, the policies and initiatives included in the upcoming Strategy need to be implemented at speed, scale and with purpose – anything less will see us move towards 2030 without substantive progress.

KPMG's submission calls out opportunities to address challenges, such as developing measurable cyber security goals and the establishment of a range of metrics that could be utilised by government to measure the success of a cyber security uplift in response. There are several regulatory and policy frameworks that institute both overlapping and incomplete security-related obligations and standards for cyber risk management. A fragmented and complex regulatory approach does not support and drive organisations to effectively address cyber risks. KPMG's submission builds on our recent response to the Review of the Privacy Act[2] which recommends that policymakers closely consider outcomes of both reviews given their overlapping remits. This submission examines mandatory reporting of cyber incidents, cyber risk through a geopolitical lens and measures to boost Australia's cyber security workforce, the latter often a key inhibiter for investing in cyber security.

We stand ready to help our clients, governments and the community be prepared for the unique cyber security challenges identified in the discussion paper and look forward to working with the Government in strengthening Australia's cyber security capability.

Yours sincerely,

Martijn Verbree
Lead Partner, Cyber Security
KPMG Australia

Greg Miller
Lead Partner, Government Cyber & Critical Infrastructure
KPMG Australia

[1] Strengthening Australia's cyber security regulations and incentives (kpmg.com)
[2] Privacy Act Review report – KPMG Submission - KPMG Australia

Background

About KPMG

KPMG is a global organisation of independent professional firms, providing a full range of services to organisations across a wide range of industries, governments and not-for-profit sectors. We operate in 143 countries and territories and have more than 265,000 partners and employees working in member firms around the world. In Australia, KPMG has a long tradition of professionalism and integrity combined with our dynamic approach to advising clients in a digital-driven world.

KPMG Cyber Security Services

As a leading provider and implementer of cyber security, KPMG knows how to apply leading security practices and build new ones that are fit for purpose. Our innovative approach to cyber security also includes the ways we deliver our services and clients can expect to work with extraordinary people who understand business and technology.

In addition to assessing cyber security and aligning it to business priorities, we help develop advanced approaches, monitor ongoing risks and help respond effectively to cyber incidents. So, no matter where our stakeholders are on the cyber security journey, KPMG helps our stakeholders reach their destination.[3]

KPMG Law

KPMG Law focuses on bringing together multidisciplinary legal teams with deep local and international experience to tackle challenging current and emerging legal and regulatory issues our clients face. With access to some of the world's leading subject matter experts on key issues such as privacy and data protection regulation, financial services, audit, tax and international transactions, KPMG Law professionals consistently bring a holistic and integrated approach to projects.

KPMG Law works with clients across multiple sectors including government, technology, education, media, telecommunications, life sciences, pharmaceuticals, energy and resources, aerospace and defence, financial services, private equity, sports and entertainment and retail sectors.

[3] https://home.kpmg/au/en/home/services/advisory/management-consulting/technology/kpmg-powered-enterprise/cyber.html

Section 1:
KPMG recommendations

RECOMMENDATION 1:

The 2030 strategy should provide Australia the opportunity to transition from its current state to a more secure position for government, industry and wider society. In pursuing this, the government should seek to develop measurable cyber security goals and metrics that must also consider emerging technologies and be able to adapt to newfound threats and adversaries. Government should be an exemplar to industry through strong leadership and the development of an ambitious reform agenda to harden government systems.

RECOMMENDATION 2:

KPMG considers the current cyber security-related regulations are a good baseline and expect that the Review of Australia's Privacy Act and other reform underway will ensure the currency of the regulations. We note that despite the ongoing gaps, there are already a large number of applicable regulations and growing number of regulators. Navigating the complexities of the environment is difficult. To improve the understanding of the applicability of legislation and regulation we suggest that clear definition of roles and responsibilities of regulators and legislation associated with mandatory reporting requirements be established.

RECOMMENDATION 3:

The *Telecommunications Sector Security reforms* and the *Security of Critical Infrastructure Act 2018* (SOCI Act) amendments seek to uplift security resilience, including cyber, across critical infrastructure sectors. The Australian Government should consider reviewing how customer data is more explicitly captured across critical sectors.

RECOMMENDATION 4:

KPMG considers that there is value in the Australian Government continuing to provide and support development of training workshops and implementation guidelines for small and medium organisations to assist in their cyber risk management.

RECOMMENDATION 5:

KPMG considers there is value in a focused effort to harmonise and fill the gaps in the current legislative landscape. A publicly-releasable stocktake of existing legislation and regulation – identifying gaps and duplication – could inform whether a dedicated Cyber Security Act or a program of legislative reform would most expeditiously achieve the outcome of clarifying, harmonising and connecting the existing legislative framework.

RECOMMENDATION 6:

KPMG recommends that the government carefully consider the risks associated with an express legislative ban on ransomware payments. Any legislative ban on ransomware payments should consider appropriate education and support schemes and whether a ban should be progressed in partnership with like countries (e.g., across the Five Eyes partnership). Any legislative ban would need to incorporate exemptions to allow for the payment of a ransom in exceptional circumstances. For example, where there was an immediate risk to health and safety.

RECOMMENDATION 7:

It is important to consider the impact of geopolitics on the cyber threat environment when formulating frameworks that incentivise the update in cyber investment. Policy makers should redouble efforts to clearly articulate the impact of geopolitics on the cyber threat and risk environment to businesses of all sizes. From our vantage point, the threats and risks are still not well appreciated. A better understanding of the threats and potential consequence should drive incentives for businesses of all sizes to understand and plan for geopolitical risk. Australia should continue its strong partnership with the Five Eyes intelligence alliance and other regional partners given cyber-attackers know no jurisdictional boundary, but also consider broader regional security partnerships.

RECOMMENDATION 8:

KPMG recommends that an independent non-profit body, similar to AusCERT, be established as a hub for sharing information about the cyber threat environment. This information sharing hub should work to collate information shared from multiple sources and manage the information securely and in a way that maintains the anonymity of the organisations providing the information. Timely and meaningful threat information sharing is still a gap in the market that existing efforts are yet to fill.

RECOMMENDATION 9:

For policy makers to understand the true impact of cyber incidents on the community, and for organisations to make informed decisions, KPMG supports proposed mandatory notification requirements to compel all organisations to report significant cyber-attacks. The Australian Cyber Security Centre (ACSC) could consider publishing reporting thresholds annually to help organisations gain a greater sense of what 'significant' means in this dynamic field.

RECOMMENDATION 10:

KPMG suggests the government – either directly or through a market-based mechanism – provides early protection of ICT assets. This could be implemented as protected DNS at the ISP level and or managed lists of known bad phone numbers to block SMS and telephone calls at the service provider.

RECOMMENDATION 11:

The Australian Government could expand current workforce and community education programs to create new pathways to build cyber talent focused on school-leavers, tertiary degree holders, and small-to-medium-sized enterprise managers, as well as incentivise the private sector to actively promote and invest in cyber skills and their cyber professionals with lifelong training programs. The Australian Government could create programs that seek to diversify company hiring processes to include a more holistic assessment of cyber candidates based on personal characteristics such as resilience, curiosity, and problem solving.

RECOMMENDATION 12:

To address the imminent shortfall of cyber security jobs in the future, Australia should consider:

- making the entry of specialised migrant workers a smoother process;
- standardising education programs;
- applying the newly released standard job descriptions for all cyber related employment positions;
- incentivising cyber education or internships in companies;
- establish a Government cyber academy to grow the pipeline of security-cleared cyber professionals across the Commonwealth, Defence and even State and Territory governments; and
- boosting the involvement of individuals in short courses and longer-term degrees.

RECOMMENDATION 13:

KPMG recommends that the Australian Government increase the scope and scale of cyber wargaming and crisis management exercises across key sectors to increase the overall preparedness of these sectors, but also ensure that organisations and the Australian Government are more aligned in certain decision-making processes, identify process gaps to be remediated, ensuring the effective protection of Australians from major cyber incidents. Promulgation of these processes to designated personnel from across the economy will be critical to build national preparedness.

RECOMMENDATION 14:

KPMG recommends that the government establish a major incident review board, co-led by government and industry board that could provide a more independent and consistent approach to understanding the root causes of major incidents.

RECOMMENDATION 15:

KPMG supports a concerted effort to draft standards and lead sector-specific implementation with leading business experts and representatives. This initiative would involve scanning global best practices and developing fit-for-purpose local arrangements in order to ensure best in class standards are developed for identifying, remediating and patching for cyber breach impacts as well as providing support to the victims of these incidents. The Government should consider funding industry to lead this work in recognition of traditional efforts making incremental progress while the threat environment has worsened exponentially.

RECOMMENDATION 16:

KPMG supports cyber health checks for small businesses given SME represent a significant portion of the Australian economy, but do not have the same level of resources to address the threat landscape. They also have the potential to collect and process large amounts of data depending on the nature of the products and services they provide. The ASX200 Health Checks from the 2016 Strategy were a useful initiative that should be repeated and could be modified for small business.

RECOMMENDATION 17:

KPMG suggests the National Reconstruction Fund could be expanded (or something similar be established) to include investment in cyber security. Substantive and ongoing investment will help grow a sovereign cyber capability, strengthen Australia against cyber-attacks, enhance resilience and ensure the continuity of services.

RECOMMENDATION 18:

KPMG recommend that the government encourage and incentivise industry and academia towards investment in research and development, ahead or in line with the curve of emerging technology. This should be led by a federal government agency or government sponsored industry partner that can facilitate trusted and meaningful information sharing. International advocacy and domestic legal accountabilities should be pursued as a priority to drive secure by design and deployment.

RECOMMENDATION 19:

KPMG supports a minimum baseline requirement for IoT, and ICS devices used in smart homes and smart cities that balances security and consumer experience. Immediate and significant investment should be made in the development of standards, appropriate use guidelines for the use of emerging technologies such as Quantum computing, Artificial Intelligence and web 3 (block chain, Metaverse) to manage potential harm to the society. A market mechanism could be considered to make quicker progress in standards development and implementation.

RECOMMENDATION 20:

To measure the effectiveness of national cyber readiness it is important to note the required outcome prior to metrics being selected. KPMG has suggested a range of metrics that could be utilised by government to measure the success of a cyber security uplift in response to Question 20.

RECOMMENDATION 21:

To support ongoing public transparency and input regarding the implementation of the strategy KPMG recommend that a feedback loop be created and implemented. This should include focus groups with general public and cyber security subject matter experts and short surveys to key enablers of the strategy.

Section 2:
KPMG insights

KPMG insights

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

KPMG views this strategy as an opportunity to establish a principle-based approach that will enable Australia to become the most cyber secure nation in the world by 2030. KPMG welcomes this sort of ambition from the Government. However, considering today's cyber security posture, Australia will need a transformative approach to achieve this ambitious objective. KPMG would like to see the following five features included:

- Transparent measures of success against which progress can be assessed and give the Australian community (and its adversaries) confidence in the agenda;
- A deliberate program of implementation that seeks to make significant early gains and therefore momentum. Investments and reforms that provides the strongest base on which to achieve the 2030 objective in the 'out years' of the Strategy should be prioritised, noting specific measures will emerge or be obsolete over time;
- In-built agility to allow for evolution in the threat environment and technology landscape;
- Clarity, standards, and incentives to enable organisations to do the right thing and induce a collaborative yet competitive behaviour among stakeholders; and
- Clear leadership by the Government to coordinate, collaborate, lead and deliver the cyber security reform agenda of Australia.

The current state

In recent years, Australia has witnessed several incidents of data breaches in addition to an increased threat from state-based threat actors on our critical infrastructure. At the same time, there is currently no clear Australian cyber security law or set of regulations. There are instead several regulatory and policy frameworks that currently institute at times overlapping security related obligations and standards for cyber risk management.

The National Cyber Security Index (NCSI)[4], which measures the preparedness of countries to prevent cyber threats and manage cyber incidents based on their documented policies, ranks Australia at 40th in the world. We note that this ranking is misleading, as countries with a lower level of digital development can achieve better cyber security scores. When compared against the countries with equal or higher digital development, Australia is ranked 12th globally, with poor performance on a few indicators. While these indicators provide some insight, they are not necessarily the only indicators on which Australia might want to be evaluated. Therefore, it is necessary to define the measurable indicators to assess Australia's performance.

The pervasive nature of 'cyber' has meant cyber security legislation and regulation has been fraught and therefore fragmented. Stop-gap measures and single-issue solutions have created a complex but piecemeal environment, readily and consistently exploited. The somewhat Defence-centric policies, standards and practices, now bolstered by the critical infrastructure protections are absolutely vital investments in our national security and resilience. However, the 2030 ambition demands an economy-wide approach to cyber security standards, policies, procedures, and guidelines.

The future state

By 2030, Australia as one of the most cyber secure nations in the world will have to have clear and consistent regulations that strengthen Australia's collective ability to prevent, deter, detect, respond to, and recover from, cyber incidents, as well as enable greater commercial and market opportunities.

Our security is only as strong as the weakest link. Therefore, Australia will assume a holistic approach of using regulations, standards, policies, guidelines and procedures across government, industry and society; across information and infrastructure assets; and all stages of the data lifecycle being

[4] https://ncsi.ega.ee/methodology/

collection/creation, use, dissemination and destruction.

While achieving the cyber security goals, Australia will not go backwards in its Digital Development Level (DDL). In contrast, it will have policies to lead the information technology industry growth through secure by design principle. Consequently, its NCSI and DDL scores will be better than that of top performing nations including Greece and Germany. Moreover, Australia will have developed measurable indicators of success that are monitored regularly. It will also continuously find and improve weakest links. Australia will have to embark on a long journey to achieve this vision.

The transition

The pathway to achieving the 2030 goals requires significant reform and action. Measurement is critical to achieving improvement, and therefore the *strategy* should start by defining and developing quantifiable cybersecurity metrics and answer questions such as how they will be measured, who will do it, and how frequently it will be measured. This activity will need to be funded and prioritised.

Australia already faces severe cyber threats and weathers successful attacks. A slow or piecemeal implementation of this strategy will leave its economy vulnerable to frequent attacks and further losses. Therefore, the strategy should consider quick win actions that will have a significant improvement on outcomes. It may be useful to consider the Pareto principle or 80/20 rule to achieve over 80 percent outcomes with 20 percent effort. The strategy will have to deliver significant outcomes within the first few years and continue improving over the following years.

While embarking on this journey, Australia's security threat landscape will continue to change. Furthermore, emerging technologies such as AI, 6G and Quantum Computing have the potential to become new threat vectors and make existing risk mitigation measures ineffective. Therefore, the strategy will have to be agile and should evaluate and improve progress over time, accommodating new changes required to tackle new threats.

In economic terms, security could be considered as public goods, which are known to suffer from the free rider problem: *everyone wants cyber security, but no one wants to pay for it*. Similarly, when a problem is everyone's problem, then it is no one's problem. This strategy will have to address these problems and provide the right balance of incentives to enable competition towards achieving the defined goals, with collaborative behaviour to help others achieve the goals and learn from others' mistakes. The strategy will also have to establish clear leadership and structures involving both the government and the private sector and make them responsible of implementing the reform agenda and achieving the goal.

RECOMMENDATION 1

The 2030 strategy should provide Australia the opportunity to transition from its current state to a more secure position for government, industry and wider society. In pursuing this, the government should seek to develop measurable cyber security goals and metrics that must also consider emerging technologies and be able to adapt to newfound threats and adversaries. Government should be an exemplar to industry through strong leadership and the development of an ambitious reform agenda to harden government systems.

2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

a) What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g., legislation, regulation, or further regulatory guidance)?

KPMG's view is that a clear set of cyber security regulatory reforms should drive practices that strengthen Australia's collective ability to prevent, deter, detect, respond and recover from cyber incidents and enable greater commercial and market opportunities. Ambition for a high-performing and competitive cyber security industry will also have positive flow-on effects throughout the Australian economy. Cyber security regulatory reforms across the economy will create demand for cyber security and related services, and thus support the acceleration of Australia's cyber security industry, but we must have the workforce ready to take up the challenge.

It is fair to say there is confusion associated with the existing legislative and regulatory environment, and at the same time there is a desire for greater regulatory clarity. While the focus on cyber by many governments and agencies is welcome, there is a need for leadership, harmonisation and filling the gaps. Active regulation and enforcement of said regulation is absolutely necessary, but governments could usefully strive for clarity among regulators and a steady march, in line with global practices.

Privacy protection is synonymous with cyber security, but there is not a linear relationship between the two. Protective obligations must be further applied across the data lifecycle – from data creation and collection to retention and destruction. This is reflected in the Australian Privacy Principles which assure a reasonable step standard to the data security obligations regulated organisations have. Of course, not all of an organisation's data, software and systems will involve the processing of personal or employee data.

Reforms as a result of the current Review of the Privacy Act should be given consideration as part of the cyber regulatory reform program. The review is wide ranging and the questions that have been posed include whether exemptions like the small business and employee records exemptions should be removed and whether the Notifiable Data Breach Scheme is effective. Other issues flagged in the review process include the emergence of digital identity and the protection of new types of personal information.

All these issues are relevant to the strengthening of the overarching cyber security regulatory framework, but they should not be considered in isolation and a thorough regulatory impact assessment process should be undertaken to ensure benefits exceed the cost of compliance. KPMG's submission in response to the Privacy Review Act sets out these recommendations in detail and should be considered alongside this submission.[5]

RECOMMENDATION 2

KPMG considers the current cyber security-related regulations are a good baseline and expect that the Review of Australia's Privacy Act and other reform underway will ensure the currency of the regulations. We note that despite the ongoing gaps, there are already a large number of applicable regulations and growing number of regulators. Navigating the complexities of the environment is difficult. To improve the understanding of the applicability of legislation and regulation we suggest that clear definition of roles and responsibilities of regulators and legislation associated with mandatory reporting requirements be established.

b) Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

Uplift of critical infrastructure regulatory framework

The discussion paper recognises that Australia's critical systems need to address vulnerabilities in supply chain security, control systems, and operational technology.[6] Australia's security approach to critical infrastructure was enhanced through legislative amendments to the *Security of Critical Infrastructure Act 2018* (SOCI Act) in 2021 and 2022. This included expansion of critical infrastructure to a wider range of sectors including: communications; financial services and markets; data storage or processing; defence industry; higher education and research; energy; food and grocery; health care and medical; space technology; transport; and water and sewerage. This provides coverage over several critical areas of the economy.

Customer data is a valuable and sensitive asset that is collected, stored, and used by various critical businesses and organisations. Customer data includes sensitive personal and financial information that, if compromised, can result in damages to individuals, businesses, and organisations.

Whilst SOCI is primarily focused on minimising risks from operational disruptions, personal information is caught by the regime under the category of the Data Storage and Processing asset class. This places obligations on those data storage and processing providers, where the service is for another critical infrastructure entity and relates to business-critical data, for which the definition includes, among other things, personal information of at least 20,000 individuals (as defined by the Privacy Act). Further, the Act does require consideration of impacts where personal information is compromised, however, it is not an explicit focus.

We believe it may be necessary to include customer data more explicitly in the ongoing reform of Critical Infrastructure through the SOCI Act to reinforce protection from cyber threats and strengthen Australia's cyber security nationally. This will provide a legal and regulatory framework to ensure that organisations responsible for collecting and

[5] https://kpmg.com/au/en/home/insights/2023/04/privacy-act-review-report-kpmg-submission.html

[6] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems

managing customer data take appropriate measures to safeguard it against potential threats. It would also allow for incident management in the case of a significant data breach.

The Privacy Act will work alongside SOCI to continue to create stronger protections under the 13 Australian Privacy Principles for how customer data is to be handled, with higher standards operating alongside SOCI for some categories of data under the existing Privacy Act.

A review of how customer data is captured under the SOCI Act would help in enhancing the trust of customers and investors in businesses following major, high-profile data breaches in Australia across 2022.

RECOMMENDATION 3

The *Telecommunications Sector Security reforms* and the *Security of Critical Infrastructure Act 2018* (SOCI Act) amendments seek to uplift security resilience, including cyber, across critical infrastructure sectors. The Australian Government should consider reviewing how customer data is more explicitly captured across critical sectors.

c) Should the obligations of company directors specifically address cyber security risks and consequences?

KPMG considers there is a need for ongoing education of company directors in order to better understand their obligations and the obligations on their management teams when it comes to cyber security risks. Education should help them achieve a level of clarity regarding the nature of cyber risk to them and what they need to do, however any education needs to be pragmatic, actionable and simple for a non-technical user to understand.

RECOMMENDATION 4

KPMG considers that there is value in the Australian Government continuing to provide and support development of training workshops and implementation guidelines for small and medium organisations to assist in their cyber risk management.

d) Should Australia consider a Cyber Security Act, and what should this include?

Currently, there is industry confusion between multiple legislative and regulatory requirements on how businesses and organisations should deal with and handle cyber security. This disconnect between the government and industry can lead to opportunities for best practice to be overlooked.

A Cyber Security Act may provide an opportunity to fill gaps in legislation, remove overlapping regulation and provide clarity to businesses. The Privacy Act would continue to apply to regulated personal information. However, there is room for greater harmonisation and filling in gaps. This could be achieved through a dedicated Act or alternatively via legislative harmonisation informed by a process of baselining and reviewing existing relevant legislation.

If a Cyber Security Act is developed, it should be done so having regard to the Security of Critical Infrastructure Act. Any proposed Cyber Security Act should provide improved coverage for businesses not currently regulated. A Cyber Security Act could provide a broader harmonisation of legislation to reduce industry confusion and overall security burden.

If the government were to consider a Cyber Security Act, the following should be considered:

- **Definitions and standards:** Clear definitions of sensitive information (in line with the (updated) definitions in the Privacy Act), data breaches, notifiable data breaches and cyber security threats should be included. Standards and guidelines for best security practices and protocols for all organisations should also be established.
- **Incident response and reporting:** A well-defined process for reporting security incidents and breaches should be included and the threshold for these made clear. Standards and guidelines for notifying affected parties, such as customers or employees, and the authorities involved.
- **Penalties for non-compliance for businesses:** Defined penalties and breaches for non-compliance with the Cyber Security Act should be considered.
- **Cyber security awareness and education:** Defined training requirements and courses for employees, vendors, and contractors should be included to ensure

the best cyber security practice and handling of incidents.

- **Information/data handling and storage:** Establishing a framework for handling, storing and sharing information between government, private organisations, and others. This will ensure best practices with information storage and sharing.
- **Privacy protections:** Alignment with the Privacy Act in relation to measures that protect personal data and privacy.
- **Incident investigation and recovery:** Procedures for investigating and recovering from cyber security incidents should be established, including mechanisms for tracing the source and best practices for recovering during a cyber security incident.
- **Monitoring and risk assessment:** Guidelines on continuous monitoring and regular risk assessments of information systems and networks should be included to prevent future security breaches.

RECOMMENDATION 5

KPMG considers there is value in a focused effort to harmonise and fill the gaps in the current legislative landscape. A publicly-releasable stocktake of existing legislation and regulation – identifying gaps and duplication – could inform whether a dedicated Cyber Security Act or a program of legislative reform would most expeditiously achieve the outcome of clarifying, harmonising and connecting the existing legislative framework.

e) How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

The government can usefully establish a cross-departmental body to monitor the impost of cyber-related regulation. The legislative and regulatory environment is, in large part, a by-product of portfolio demarcations. The collective of relevant policy departments should hear the practical implications of adjacent or overlapping reforms. Industries should equally be encouraged to work collaboratively to help inform government.

f) Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances?

i) What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

g) Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

In response to f) and g), KPMG understands that policy makers in Australia and internationally are considering regulatory options to address the payment of ransoms demanded following ransomware attacks, given these payments incentivise cyber criminals and could breach anti-money laundering and counter terrorism financing (AML/CTF) laws.

KPMG recommends that the government carefully consider the risks associated with an express legislative ban on ransomware or extortion payments. Any legislative ban on ransomware payments should consider appropriate education and support schemes and whether a ban should be progressed in partnership with like countries (e.g., across the Five Eyes partnership). The legislative ban will need to incorporate exemptions to provide for the payment of a ransom in exceptional circumstances, such as immediate risks to health and safety. In addition, policy makers need to carefully consider whether a ban would create incentives for organisations to under report or attempt to conceal ransomware attacks given the potential significant financial and operational impacts of not paying a ransom in some scenarios. This would be counterproductive given the government is trying to incentivise incident reporting and the sharing of threat information.

We understand the United States and European Union have taken steps on regulation of ransomware payments, including a sanctions list and sector-based regimes. Australia could look to these countries to inform its approach. A 2020 ruling by the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN) states most cases of paying a ransom are illegal. The EU has taken a similar path when it comes to what are deemed "essential services," which they have recently

expanded. EU member states can impose fines for paying ransoms under the Security of Network and Information Systems Directive (NIS Directive).

When assessing policy options for mandatory disclosure of and restrictions in relation to paying ransoms, it is important to remember that governments are not immune to cybercrime, including ransomware attacks. Any efforts to lift resilience and security in the economy will need to be matched with actions taken by government organisations. Governments must lead by example, both in protecting against cybercrime but also in how they respond to attacks. Any new regulation must also apply to government and the public sector.

Governments and larger businesses will also have a key role in helping smaller businesses lift their cyber security. The services and software products of smaller businesses can be critical in the connected digital supply chain, but they may not have the capability or resources to adequately protect themselves or recover from a successful attack which could also impact on government and bigger business customers. Therefore, government support that focuses on lifting the cyber security and resilience of smaller businesses is required as part of any approach to tackling ransomware attacks.

Lastly, addressing ransomware will need to be part of a broader effort to both tackle cybercrime and to improve the overall cyber security posture of Australian businesses, large and small, as well as government. While ransomware has grown in prominence in recent years, we encourage the government to tackle it through a broader cybercrime and cyber security framework. A holistic response to ransomware will need to come from across the policy spectrum, from securing systems through to deterrence, including law enforcement.

RECOMMENDATION 6

KPMG recommends that the government carefully consider the risks associated with an express legislative ban on ransomware payments. Any legislative ban on ransomware payments should consider appropriate education and support schemes and whether a ban should be progressed in partnership with like countries (e.g., across the Five Eyes partnership). Any legislative ban would need to incorporate exemptions to allow for the payment of a ransom in exceptional circumstances. For example, where there was an immediate risk to health and safety.

3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?

4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?

Cyberattacks know no borders, and with the interconnectedness of global digital infrastructure in today's world, large cyberattacks affecting multiple countries are becoming increasingly common. In addition, with the rapidly shifting geopolitical and strategic landscape, cyber espionage is increasing in frequency and scale, with the potential for a single cyberattack to compromise multiple countries. As such, it is critical for Australia to have robust mechanisms for cyber cooperation with regional and global partners to ensure mutual cyber resilience. Conventional warfare also increases cyber risks, and geographical isolation does little to reduce vulnerability. The recent increase in sanctions on Russia has seen a corresponding uptick in cyber-attacks. Future conflicts elsewhere in the world could result in further cyber insecurity.

Australia currently has various tools for international cooperation in regard to cyber security. The Department of Foreign Affairs and Trade currently leads Australia's international engagement on cyber and critical information technology, is coordinated by the Australian Ambassador for Cyber Affairs and Critical Technology, and is a member of the ASEAN Regional Forum's ICT work stream. Australia's Cyber and Critical Tech Cooperation Program was additionally established in 2016, and expanded in 2021 to include cooperation on critical infrastructure, to foster the development and improvement of cyber resilience throughout the Indo-Pacific region, and includes 26 regional partners to pool knowledge and resources to boost the collective cyber resilience of the region.

There has been collaboration with the UK under the Cyber and Critical Technology Partnership, which provides a forum for both countries to discuss cyber capacity building between countries and across the broader Indo-Pacific. The Partnership also aims to enhance cyber security and resilience while ensuring reliable access to the opportunities provided by the rapidly expanding digital economy. Cyber has also had an increased presence at the annual Australia-UK Ministerial Consultations (AUKMIN). Additionally, Australia has an

agreement with Singapore in the form of a bilateral Memorandum of Understanding (MoU) on Cyber Security Cooperation which will be in place until 2025. The MoU gives both countries the opportunity to work together in the management of cyber threats. Australia's International Cyber and Critical Technology Engagement Strategy includes $17 million to help Pacific nations fight cybercrime, improve online safety, and counter disinformation and misinformation. And the Australian government-funded Pacific Cyber Security Operational Network (PaCSON) has established cyber-incident response officials throughout the Pacific region.

Many of the agreements Australia has for international cyber cooperation and cooperative defence are at the government and critical infrastructure level. Given this, it is possible that some benefits such as shared knowledge, resources, and information may not necessarily trickle down to the small and medium sized businesses. There is an opportunity to better arm these businesses with the resources and knowledge required to uplift their resilience. This becomes particularly important in instances where cyber threat actors working on behalf of nation states target their cyberattacks on entities that are a critical part of the supply chain for both government entities as well as smaller and medium businesses.

In order to combat this and enhance the resilience of the small and medium sized businesses, Australia's international engagement should not only use its existing multilateral and bilateral engagements to boost cyber to enhance cyber resilience and response processes for government and critical infrastructure organisations, but also to ensure that small and medium enterprises in the region and partner countries have the knowledge, awareness, and resources to protect themselves from cyber risks and threats which continue to emerge and evolve along with the global geopolitical landscape. To fully engage small and medium sized businesses, bilateral and multilateral cyber arrangements and partnerships should include proactive sharing of regional cyber threat and landscape information, and do so in a way that is accessible and easily digestible for organisations of all cyber maturity levels. Additionally, capacity building grants which may be part of regional and bilateral cyber cooperation programs should prioritise projects which work to build the cyber resilience, knowledge, and awareness of small and medium sized businesses.

RECOMMENDATION 7

It is important to consider the impact of geopolitics on the cyber threat environment when formulating frameworks that incentivise the update in cyber investment. Policy makers should redouble efforts to clearly articulate the impact of geopolitics on the cyber threat and risk environment to businesses of all sizes. From our vantage point, the threats and risks are still not well appreciated. A better understanding of the threats and potential consequence should drive incentives for businesses of all sizes to understand and plan for geopolitical risk. Australia should continue its strong partnership with the Five Eyes intelligence alliance and other regional partners given cyber-attackers know no jurisdictional boundary, but also consider broader regional security partnerships.

5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?

The contested geopolitical environment raises the risk of rival standards, laws and norms emerging from the major global tech powers. As a middle power, Australia's cyber-space interests are best served by an open global rules-based order, as are its broader trade and investment interests. However, in the years ahead, pressure may grow to choose which standards and rules to align with. Standard setting efforts need to be fast-tracked and given greater prominence within government and the private sector. Government should consider how to better use industry to make meaningful progress.

Australia is already active in key standard-setting initiatives but should ensure it retains a seat at the table as these norms and rules continue to develop. The International Cyber and Critical Technology Engagement Strategy is a positive step in this direction, as is the government's support for UN efforts to set rules and norms of responsible state behaviour in cyberspace. Seeking additional opportunities to share resources and learnings with ideologically aligned nations will help Australia contribute to – and benefit from – international legal guardrails.

Some examples of forums Australia could consider engaging with include the OECD Global Forum on Digital Security for Prosperity, the UN Counter-Terrorism office's cyber security program, and the UN norms of responsible state behaviour in cyberspace.

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

It is critically important that government serves as a role model for other entities in the Australian economy. Government is yet to be that model either in design or implementation. Whatever replaces the cyber hubs initiative as the delivery function for 'hardening government IT' needs to be driven at speed. Clear leadership, sufficient centrally coordinated funding and effective governance will need to be adopted if the Commonwealth is to make substantive progress. KPMG recognises funding for this measure will be challenging in the current fiscal environment and government architecture. The Minister for Home Affairs and Cyber Security could perhaps pick up this initiative as a personal priority to drive reform across government and report on measures to harden government IT. Government has an opportunity to lead by example in this space as it works through the complex issues around legacy systems, prioritisation and funding.

7. What can government do to improve information sharing with industry on cyber threats?

Information sharing between government, academia, and industry on the cyber threat landscape and emerging trends and threats is essential to maintain a resilient and robust cyber defence posture, and ensure that organisations within Australia at risk from cyber threat actors have a thorough understanding of the threats that they face by being able to collectively understand, analyse, predict, and ultimately counter these threats.

Australia currently has a robust and multi-layered information sharing network. ACSC's Partnership Program, which is delivered through the Joint Cyber Security Centre (JCSC) network (which has a presence in key capital cities including Sydney, Melbourne, Perth, Adelaide, and Brisbane), 'enables Australian organisations and individuals to engage with the ACSC and fellow partners, drawing on collective understanding, experience, skills, and capability to lift cyber resilience across the Australian economy,' and partners gain access to threat intelligence in the form of alerts, advisories, and automated indicators, and additionally provides partners a platform to share threat intelligence with each other and the ACSC, as well as collaborate to mitigate shared challenges.[7] Additionally, the Trusted Information Sharing Network (TISN) is the mechanism through which the Australian Government engages with industry on critical infrastructure, and is made up of critical infrastructure owners and operators, supply chain entities, peak bodies, academics, and government. TISN member organisations periodically meet, and works to bring members together to enhance the security of critical infrastructure. The final major mechanism for information sharing in Australia is in the form of security bulletins and other information security services provided by AusCERT to member organisations.

Improvements can be made to the existing information sharing regime in Australia, however. In particular, it was noted in the 2016 ACSC Cyber Security Survey[8], and by MITRE[9], that one of the key reservations that organisations have in regards to information sharing is that a higher degree of trust is required between organisations before they share potentially sensitive information with each other. Having an information sharing network that has a strong, fully trusting relationship will ensure that the quality of information shared is of higher quality and enhance cooperation and stakeholder buy-in.

In order to facilitate this, an independent non-profit body, similar to AusCERT, should be established as a hub for the broader information sharing network. This information sharing hub should work to collate information shared from multiple sources and manage the information securely and in a way that maintains the anonymity of the organisations providing the information. As the cyber threat landscape has and continues to significantly grow and evolve, it will be important to ensure that the information disseminated by information sharing groups is in real time, and is actionable by and relevant to member organisations. Ensuring the relevance of shared data to member organisations can be achieved by slightly reforming the ACSC Partnership Program and AusCERT bulletins. In particular, different information sharing sub-groups should be established based on industry sectors, similar to how the TISN is structured with different groups for each critical infrastructure sector. This sub-grouping can be extended to the JCSC Network to take advantage of the industry groups which are dominant in each city in which the JCSC has a physical presence – for example, Perth may specialise in information and cyber threats specific or more relevant to the mining and resources sector.

[7] ACSC Partnership Program | Cyber.gov.au
[8] 2016 Cyber Security Survey (apo.org.au)
[9] Building a National Cyber Information-Sharing Ecosystem (mitre.org)

RECOMMENDATION 8

KPMG recommends that an independent non-profit body, similar to AusCERT, be established as a hub for sharing information about the cyber threat environment. This information sharing hub should work to collate information shared from multiple sources and manage the information securely and in a way that maintains the anonymity of the organisations providing the information. Timely and meaningful threat information sharing is still a gap in the market that existing efforts are yet to fill.

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

KPMG considers that it is important to take into account the confidentiality needs of impacted organisations to be protected from reputational damage as well as exposure to the further risk of targeted attacks. Confidentiality will encourage voluntary incident reporting. The potential for organisations to be identified or for their confidential information to be disclosed as part of a cyber incident report, may inhibit voluntary reporting. KPMG considers that there can be a better balance struck between transparency and data anonymisation that seeks to achieve the public policy objective of intelligence gathering and remediating harm caused by breaches, while also limiting the cost through reputational damage.

This information could help government and businesses make informed decisions about their digital and cyber security investments as well as the development of targeted policy approaches. It would also demonstrate if regulatory reforms and business practices are having any impact on reducing the number of cyber incidents. KPMG supports incentives for organisations that do voluntarily report incidents, given the additional investment organisations are making to do so.

Mandatory incident reporting as required under the SOCI Act has different considerations in relation to privacy and confidentiality. Where an incident is reported to ASCS, it would be expected that this information was passed onto the regulator (Home Affairs) in line with the respective legislation, except when it falls under the definition of protected information within the Act.

9. Would expanding the existing regime for notification of cyber security incidents (e.g., to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

The incidence of cybercrime is currently measured through voluntary reports made by individuals and business to the ACSC, with mandatory reports required under the same mechanism for entities captured by the Security of Critical Infrastructure Act 2018 (SOCI). Further, certain data breaches must be reported under the NDB Scheme in the Privacy Act and the individual reports and complaints to the ACMA, the ACCC and IDCare. The ACSC and other agencies use this information to produce public alerts and advisories, inform threat reports and provide guidance to the community.

Currently the NDB Scheme in the Privacy Act, which was one of the first of its kind to be introduced, requires regulated private sector organisations and Commonwealth agencies to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) of a data breach that is likely to result in serious harm to any individual whose personal information is involved[10] - that is an 'eligible data breach'. If an organisation or agency suspects an eligible data breach may have occurred, they have positive obligations to quickly investigate and assess the incident to determine if it is likely to result in serious harm to any individual and is therefore notifiable.

The OAIC publishes bi-annual reports on the data breaches notified to it. These reports provide some insights into sectors and the number of individuals affected, root cause and trends (such as ransomware), as well as effective breach responses, to help organisations prepare for and manage data breaches. However, this information is limited and does not detail the cost of breaches or provide deeper insights into the root causes and response, that would benefit organisations and agencies. This in part reflects the prescribed information that must be included in the

[10] https://www.oaic.gov.au/privacy/notifiable-data-breaches/

notification report. It is also limited by the exemptions that currently apply in the Privacy Act which mean the NDB scheme does not currently cover smaller businesses and employee records.

In the US, all 50 states have enacted legislation requiring private or governmental organisations to notify individuals of security breaches of information involving personally identifiable information.[11] Security breach laws typically have provisions regarding who must comply with the law, definitions of personal information, what constitutes a breach, requirements for notice, and any exemptions.

While the notifiable data breach schemes globally provide policy makers with knowledge of cyber incidents that result in loss of personal data, there is no notifiable regime for general cyber-attacks that seek to access to corporate information and/or cause operational disruption or extract a financial gain. However, this is starting to change, as noted above (e.g., including through mandatory reporting for entities captured by the SOCI Act). It is also understandable that some organisations choose not to report cyber incidents. The reasons for this can include a lack of information around what is considered significant to authorities and/or whether it is captured as part of the current notifiable regimes, but also because of the potential for significant reputational damage. The government can address this by building trust with the business community and providing assurances that it will not publicly disclose names of victim organisations and their reporting data will remain confidential.

For policy makers to understand the true impact of cyber incidents on the community, on organisations and on the Australian economy, KPMG supports proposed mandatory notification requirements to encourage all organisations to report cyber-attacks. Cyber incidents can have consequential impacts throughout the economy. Early detection and reporting to the ACSC could help the ACSC for example, alert the community quickly about new threats. Using this information, organisations can take swift defensive measures to protect their systems. As part of this effort, the ACSC could consider publishing reporting thresholds annually to help organisations gain a greater sense of what 'significant' means in this dynamic field.

KPMG supports further work to estimate the economic impact of cyber incidents to Australia given the current data limitations. In the long-term, mandatory reporting should consider including estimates of business cost to ensure the full economic story is known. If governments and businesses better understand the full economic cost, then resources can be better targeted to address the size and nature of the problem.

RECOMMENDATION 9

For policy makers to understand the true impact of cyber incidents on the community, and for organisations to make informed decisions, KPMG supports proposed mandatory notification requirements to compel all organisations to report significant cyber-attacks. The Australian Cyber Security Centre (ACSC) could consider publishing reporting thresholds annually to help organisations gain a greater sense of what 'significant' means in this dynamic field.

10. What best practice models are available for automated threat-blocking at scale?

There are multiple ways to conduct automated threat blocking and management at a larger scale. These include encouraging and incentivising businesses to utilise a passive domain name system (DNS), and Internet Service Provider (ISP)-level blocking of malicious web content.

The Australian Protective Domain Name Service (AUPDNS) protective DNS made available to Australian Government agencies through the ACSC, or another such protective DNS, should be incorporated into the ACSC Partnership Program and be additionally made available to Australian businesses who wish to utilise it. The protective DNS will work to automatically check inbound and outbound network traffic against known high-risk websites and email servers, with high-risk traffic being blocked.

ISPs and telecommunication companies in Australia should additionally implement web filtering of malicious content. As malicious advertisements and URLs are the primary vector used by cyber threat actors to spread malware, having ISPs implement a web filter to block known malicious URLs would significantly cut the number of potential phishing attacks affecting individuals.

A further method of managing threats to individuals, while not automated, would be to improve the existing method of reporting cyber

[11] https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

incidents to the ACSC. A mobile app could be utilised to block scam calls and SMS messages by comparing the phone number of an incoming call to a list maintained by the ACSC of known phone numbers used to make these scam calls, with those that are a match being blocked, and users should be given an option to report scam phone numbers that were missed, which would then be analysed by the ACSC.

Currently, some telecommunication and financial institutions have mechanisms for reporting scam calls and SMS messages however reporting mechanisms are not always intuitive to individuals, and many individuals may not even be aware of any such reporting mechanisms. Having the ACSC maintain a centralised blocklist, and one which individuals and organisations can add to by reporting scam calls and SMS messages to the ACSC, will ensure scams are blocked on a large scale. This approach has been used successfully in Singapore, with the National Crime Prevention Council (NCPC) and Singapore Police Force-managed ScamShield app, which blocked over 24,000 phone numbers utilised by scammers, and saw 5.1 million SMS messages reported between its launch in November 2020 and August 2022.[12]

RECOMMENDATION 10

KPMG suggests the government – either directly or through a market-based mechanism – provides early protection of ICT assets. This could be implemented as protected DNS at the ISP level and or managed lists of known bad phone numbers to block SMS and telephone calls at the service provider.

11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?

Preparing a future pipeline of cyber graduates

Introducing cyber security at a young age has a twofold advantage: to stimulate an interest and desire to pursue a career in cyber and, as our next generation of digital natives are immersed in a cyber world, to make their online experiences safer. According to a 2019 survey, 29 percent of CIOs interviewed stated that education is the primary factor in alleviating the IT skills shortage in Australia.[13]

Scope of the existing pipeline

In the existing pipeline of future graduates, students might show an interest in computers, investigate IT as a career, discover cyber security, follow a pathway to a tertiary qualification and then enter the workforce. The students might participate in a STEM program at school. The current Australian curriculum touches on technology, but doesn't explicitly focus on cyber security. Most primary schools' timetables only allow for immersion in technology once or twice a week[14], and high school students need to elect to study technology as a subject. At university, there are numerous cyber security options and even more IT courses available. If graduates are lucky enough to get into a graduate program, they are provided with the mentorship and experience necessary to secure a job long term, however in October 2021, only two percent of cyber security jobs were graduate level.

From this pipeline some concerns are evident. While awareness of cyber security is on the rise, this awareness isn't necessarily happening at the school level. In the National STEM School Education Strategy 2016-2026, the Education Council committed to ensure all students finish school with strong foundational knowledge in STEM and related skills, and ensure that students are inspired to take on more challenging STEM studies.[15] In terms of ICT, the council has implemented a free digital technology hub. On average, each school in Australia has only visited this site seven times a year. There are other free resources available to promote cyber security awareness and culture that also have a low utilisation.

Preparing the future pipeline

Focusing on developing a high-tech workforce requires awareness, interest, and investment in holistic education at all school levels. Introducing IT skills and cyber education has a threefold advantage for students. It stimulates a curiosity and desire to pursue a career in cyber; helps to create safer online experiences in an increasingly digital world; and cyber skills promote general capabilities in communication, literacy, and numeracy skills. Cyber security can be used in all learning areas and particularly incorporated into STEM programs. Schools can promote a safe IT culture within the school

[12] Anti-scam app ScamShield blocks 24,500 phone numbers; 5.1m SMSes reported on app | The Straits Times
[13] AU_Robert Half Press Release_IT skills shortage solution_31 May[1][2]
[14] 10. Use of technology in the classroom | Growing Up in Australia
[15] National STEM School Education Strategy - Department of Education, Australian Government

environment by incorporating exciting interactions with computers such as scavenger hunts, coding camps, and class challenges promoting cyber security as a career and framing IT safety as a function of public good.

These standardised learning pathways are critical in boosting the future pipeline. An additional resource that is needed to ensure the competitiveness of Australia's cyber security workforce is teaching staff. The lack of qualified teachers and professors is of great concern to tertiary education institutes. Funding, tax incentives, and other initiatives from government and large companies might assist in these areas.

In order to prepare a future pipeline of cyber graduates, awareness of cyber security should be promoted, and various IT careers should be showcased to students at all levels of schooling. This seed of knowledge should be developed through interactive challenges promoting cyber skills and cultivated by a resource rich tertiary education experience through a standardised education framework with availability of the required educators

RECOMMENDATION 11

The Australian Government could expand current workforce and community education programs to create new pathways to build cyber talent focused on school-leavers, tertiary degree holders, and small-to-medium-sized enterprise managers, as well as incentivise the private sector to actively promote and invest in cyber skills and their cyber professionals with lifelong training programs. The Australian Government could create programs that seek to diversify company hiring processes to include a more holistic assessment of cyber candidates based on personal characteristics such as resilience, curiosity, and problem solving.

12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

Boosting Australia's cyber workforce skills

Delivering enduring cyber resilience in Australia will require a fundamental shift in approach to developing an appropriately skilled workforce. Addressing this challenge will require workforce, labour market, and industry reforms away from the zero-sum game of competing to recruit talent towards a concerted effort to grow the workforce, skills, and industry required in the future.

In their 'Sector Competitiveness Plan', AustCyber divides the cyber workforce into two categories of people that need cyber skills: a general cyber-literate but non-specialist workforce, and a specialised workforce with technical and non-technical professional cyber security skills.[16]

In the short term, the growth in the cyber security workforce isn't meeting the demand. AustCyber has estimated a shortfall of 17,000 workers for cyber related jobs in 2026. The Information Systems Audit and Control Association (ISACA) and the International Information System Security Certification Consortium ((ISC)2) detail in their latest reports a potential global short fall of up to 2.93 million cyber security professionals.[17]

Migration to unlock overseas talent

Labour costs, our geographic remoteness from major markets and capital sources, limited local market demand, constrained supply chains, infrastructure latency and time-zone differences with major English-speaking markets continue to create barriers for attracting global cyber talent.

Most of the growth is coming from workers transitioning from other IT related jobs. Australian university graduates often do not have enough experience to fulfil the requirements of cyber jobs. One immediate solution is to make the entry of migrant workers a smoother process. An increase in skilled migrants also has the added benefit of increasing economic growth as KPMG found in a recent submission *A migration system for Australia's future*.[18]

Professional frameworks

To ensure Australia is equipped to meet the surge in cyber workforce professionals needed in 2030; policy makers have established a national benchmark for cyber education and skills framework.[19] The Australian Signals Directorate (ASD) has recently released an ASD Cyber Skills Framework which defines roles, capabilities and skills essential for ASD's cyber mission.

For professionals wanting to transition to cyber security, the ASD document gives a defined

[16] https://www.austcyber.com/resources/sector-competitiveness-plan/chapter3
[17] https://www.austcyber.com/resources/sector-competitiveness-plan/chapter3
[18] https://kpmg.com/au/en/home/insights/2023/02/migration-system-for-australia-future-kpmg-submission.html
[19] https://www.cyber.gov.au/sites/default/files/2020-09/ASD-Cyber-Skills-Framework-v2.pdf

pathway of transition. ASD has defined one learning and development pathway as an example. While ASD is not a skills, education or employment agency, this document could be expanded to include the various role definitions. This standardised education framework provides employers with assurance that individuals have the necessary skills to perform a certain job. ASD has aligned role definitions to capabilities and skill definitions and detailed six proficiency levels within these skills areas. This makes the cyber job hunt and recruitment search easier. The standardisation of cyber jobs and education leads to a clearer development pathway for individuals with guaranteed fit for purpose skills that employers are looking for.

In the US, a partnership with government, tertiary institutions and the private sector have developed the National Initiative for Cybersecurity Education (NICE) that addresses current and future cyber security education issues through the promotion of best practices. Their framework helps both employers and employees to set a standard that all can work towards. ASD has used this framework as a basis for their ASD Cyber Skills Framework.

Formal education pathways

Education is at the cornerstone of boosting cyber skills in the workforce. A cyber professional or someone wanting to transition into cyber has a choice of obtaining a degree, completing a vocational certificate, or completing an industry certification from organisations including but not limited to ISC and ISACA. There is some debate as to which is better. Degrees hone executive skills and high-level knowledge across the cyber field, whereas certificates and certifications can accurately reflect the fast-paced change of information in the cyber field and may provide more in-depth knowledge in a particular area. To encourage individuals to participate in formal cyber security education, it may be warranted to consider appropriate government incentives in the short to medium term.

Vocational education also has an important role to help re-skill members of the existing workforce, who wish to switch careers or up-skill within their current job. It can also help in providing alterative pathways for schools-leavers to enter the cyber workforce, where university may not be a viable option. TAFEs and Canberra Institute of Technology are offering excellent nationally recognised cyber education programs that can be tailored to suit individuals' personal situation. These offerings are often a highly cost-effective alternative to academic offerings or professional certifications.

Diversity in skills shortage

Within the work skills shortage, Australia has certain roles that have a higher demand than others. Investment is needed into this diversity in skills shortage, to identify roles with the most significant shortages.

Cyber requires a broad range of skills from project managers, architects, engineers, DevSecOps, specialised training, education, awareness personnel, CISO/BISO, writers (technical & content), coordinators, Security Operation Centre specialists, and threat hunters. The ASD framework addresses these skills in detail and forms a good basis for development focus areas.

One highly technical role is that of security architecture. This role provides detailed technical, professional and policy advice on security management. It requires in-depth knowledge that encompasses the entire cyber realm. The experience required to perform this job competently is extensive.

Australian policy makers might want to consider what resources are necessary to correctly address the wide variety of skills needed to successfully compete in the global cyber security economy.

Skills matching and retraining

There is also a role for the Australian Government to undertake large scale skills identification, job matching and retraining analysis in conjunction with other government partners. This should include analysis of industries currently under threat due to role automation such as in finance and accounting. Additionally, further investment in University partnerships, uplift of relevant curriculums, and leadership of diversity programs for the sector should be considered in parallel. To provide expedited capacity for the market, investment in reducing barriers to transition programs for professionals with relevant skills and advocacy for skilled migration should also be evaluated for benefits.

Industry led workforce development

Another approach to increasing cyber security skills in Australia is to incentivise education or internship programs within companies to actively promote and invest in cyber skills.

Companies could also review their hiring processes. Qualifications and certifications are important, but indications from the USA and Europe suggest a more holistic assessment of candidates based on personal characteristics such as resilience, curiosity and problem solving is important too.

Ex-members of the military and security services often have the aptitude to re-skill as cyber professionals, as do graduates holding non-STEM degrees. On the other side of every hacking attempt is a human brain trying to discover and exploit vulnerabilities, therefore being able to think from their perspective and anticipate their actions is a valuable skill.

Making cyber internships mandatory to apply for government contracts would spur big companies into making the change to boost the skills in the cyber workforce. In 2011, the Defense Advanced Research Projects Agency (DARPA) in the United States began Cyber Fast Track, a project designed to award small, short-term contracts to boutique firms and individuals with cyber skill sets needed for the DARPA mission. This initiative encouraged small businesses and individuals to upskill in the necessary skills needed for DARPA's projects. DARPA was able to harness the skills they needed in short-term contracts in order to achieve specific cyber security outcomes.

Flexible cyber roles in the regions and at home

Investing in schools and TAFEs to increase the number of people in the workforce who can meet the growing demand for cyber security expertise shouldn't just be confined to the cities. Through the COVID-19 pandemic we have learnt that remote working is an absolute possibility, and cyber security is an area that naturally lends itself to being able to be supported by a distributed workforce working from remote and regional Australia.

Policy makers should also consider tapping into the workforce of previously working parents – there are many highly educated women who cannot or do not want to return to full time work, but who find themselves unable to return to their previous jobs in a part-time capacity.

RECOMMENDATION 12

To address the imminent shortfall of cyber security jobs in the future, Australia should consider:

- making the entry of specialised migrant workers a smoother process;
- standardising education programs;
- applying the newly released standard job descriptions for all cyber related employment positions;
- incentivising cyber education or internships in companies;
- establish a Government cyber academy to grow the pipeline of security-cleared cyber professionals across the Commonwealth, Defence and even State and Territory governments; and
- boosting the involvement of individuals in short courses and longer-term degrees.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

a) Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

Streamlining incident reporting

The Australian Government should consider streamlining the existing process used by organisations and individuals to report cyber incidents. The existing ACSC reporting mechanism should be the single portal used to report incidents, with the reporting form being amended to include details required by other regulators and bodies, such as additional details for incidents involving personal information which may be required by the OAIC, or details of leaked government data as may be required to be reported under the PSPF. This is already the case for incidents required to be reported under the Security of Critical Infrastructure Act 2018 (SOCI).

Merging incident reporting forms from across regulators and government bodies will make it easier for individuals and businesses to report major incidents and eliminate the need for multiple reports to be made to different government entities. To this end, processes should be established to forward reports made to the ACSC to other relevant regulators and government bodies, such as the OAIC, based on the nature of the incident that was reported.

Improving sector-wide cyber crisis management

KPMG welcomes the recent commitment from the government to conduct sector-wide cyber crisis management and wargaming exercises

regularly and on a larger scale across the economy.[20]

Sector-wide crisis management and wargaming exercises should include regulators and representation from other relevant government bodies in addition to the major and some minor organisations operating within a given sector. Scenarios developed for these wargaming exercises should additionally be designed based on current and emerging trends in the cyber threat landscape, and in a way that thoroughly stress-tests existing protocols for communication – within organisations, between organisations, with regulators and the ACSC, and with the public – and incident response and analysis activities.

In addition to exercises testing existing sector-wide business continuity and crisis management procedures, further exercises should be conducted to focus on more granular aspects of cyber incident response that may not be uniform across organisations. This includes initial incident identification and analysis, the decision-making processes surrounding whether an incident is determined whether or not to be a 'major' cyber incident and the activation of resources following that determination. In order to effectively test this, exercises should consist of multiple scenarios that comprise of major and minor incidents, with the aim of highlighting the uncertainties inherent in cyber incidents and identifying what information is critical to ensure accurate follow-up decisions. Promulgation of these processes to designated personnel from across the economy will be critical to build national preparedness.

RECOMMENDATION 13

KPMG recommends that the Australian Government increase the scope and scale of cyber wargaming and crisis management exercises across key sectors to increase the overall preparedness of these sectors, but also ensure that organisations and the Australian Government are more aligned in certain decision-making processes, identify process gaps to be remediated, ensuring the effective protection of Australians from major cyber incidents. Promulgation of these processes to designated personnel from across the economy will be critical to build national preparedness.

14. What would an effective post-incident review and consequence management model with industry involve?

A major incident review board, co-led by government and industry, would be a positive net addition to Australia's cyber security architecture. This board could provide a more independent and consistent approach to understanding the root causes of major incidents – be they affecting public or private sector organisations – and build a catalogue over time of outstanding vulnerabilities affecting the Australian economy. Such a board could afford both governments and victim organisations an off-ramp for media interest in the 'why' and 'who is to blame' in the immediate aftermath of a cyber incident.

RECOMMENDATION 14

KPMG recommends that the government establish a major incident review board, co-led by government and industry board that could provide a more independent and consistent approach to understanding the root causes of major incidents.

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

There is currently a disconnect between government best practice behaviours and industry or society best practice. Many government-based cybersecurity standards and initiatives are targeted at government or defence systems, and therefore are not practical and incredibly difficult for wider industries such as small to medium enterprise businesses to implement. The government could seek to reduce this gap by providing a best practice response which caters to varying levels of business and system complexity.

There is an expectation gap regarding cybercrime and how to best support its many victims. Citizens are demanding more than just an identity checking service as remediation for being a victim to a cybercrime. Furthermore, we have seen how cybercrime can affect the wider population when personal health data was released last year, potentially impacting victims' employment status and clearance levels. When it comes to victim support, businesses could consider providing, for example, mental health

[20] https://www.smh.com.au/politics/federal/consider-what-damage-could-be-caused-government-launches-cyber-war-games-for-major-banks-20230410-p5czbj.html

services or cybersecurity awareness training in addition to services such as ID Care. Australia's strategy should also recognise the global push towards cyber insurance as mechanism to lower recovery costs and provide further support for victims.

RECOMMENDATION 15

KPMG supports a concerted effort to draft standards and lead sector-specific implementation with leading business experts and representatives. This initiative would involve scanning global best practices and developing fit-for-purpose local arrangements in order to ensure best in class standards are developed for identifying, remediating and patching for cyber breach impacts as well as providing support to the victims of these incidents. The Government should consider funding industry to lead this work in recognition of traditional efforts making incremental progress while the threat environment has worsened exponentially.

a) What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

Small and Medium Enterprise (SME) represent a significant portion of the Australian economy and while they experience many of the same security issues as larger enterprises, they do not have the same level of resources available to address the threat landscape. They also have the potential to collect and process large amounts of data depending on the nature of the products and services they provide.

It is in the SME sector that we need to be even more innovative to help small businesses appropriately manage their risk profiles in a way that is also sensitive to their unique context. This will not only benefit SMEs but also the larger companies for whom they are often suppliers or customers and therefore part of the supply chain.

Cyber health checks for small businesses may be a suitable way for the government to support small businesses in managing their cyber security risks.

We need to couple broad based education of the sector with the health check program so that SMEs better understand the nature of the threat landscape in which they operate and their obligations.

This then provides a sound backdrop against which to perform a health check for an SME to help them manage their own risk and those around them.

KPMG has recognised this need for SMEs to have an objective assessment of their cyber risk profile called a 'health check' undertaken, particularly in the context of the current threat landscape as it helps SMEs to identify and remediate any security control gaps and risks before an incident occurs. This may also help prioritise future investment to enhance business risk reduction. These health checks can include assessments using frameworks that have been developed based on industry standards.

The types of outcomes KPMG has identified as part of a Cyber health check include:

- An agreed risk appetite statement that reflects risk tolerance.
- A clear view of the cyber threats that an organisation may face, including external threats such as geopolitical tensions which may commonly be overlooked by SMEs.
- How these cyber threats translate into risks based on information assets combined with the control environment.
- An assessment of cyber control maturity.
- A tangible and executable roadmap of cyber uplift activities, which are prioritised based on the risk reduction.
- Incident response preparation and planning that has regard to the health check and risks identified.

From our experience of undertaking health checks the feedback has been very positive. These checks could be subsidised by the government according to a certain level of annual turnover, such as the current definition of a small business in the Privacy Act which is an annual turnover of less than AUD $3 million.

We also suggest that this be considered in conjunction with drivers to deploy privacy and security enhanced technologies. KPMG notes the current proposal in the Privacy Act Review Report to remove the small business exemption in the Privacy Act. This will have a significant impact on small businesses if implemented, and as such it is critical to consider how any further changes will interact with other aspects of the regulatory framework.

RECOMMENDATION 16

KPMG supports cyber health checks for small businesses given SME represent a significant portion of the Australian economy, but do not have the same level of resources to address the threat landscape. They also have the potential to collect and process large amounts of data

depending on the nature of the products and services they provide. The ASX200 Health Checks from the 2016 Strategy were a useful initiative that should be repeated and could be modified for small business.

16. What opportunities are available for the government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

Investing in cyber security would help to strengthen the country's defences against cyber-attacks, enhance resilience, and ensure the continuity of essential services. In return, this provides Australia with new jobs and promotes Australia to become a cyber security leader.

Developing new and somehow enforceable frameworks that clearly define and provide guidance for organisations, businesses and individuals on cybersecurity is an opportunity that provides assurance within standards. This framework will also provide enforcement operations across Australia.

Currently most of the innovative products that are founded in Australia as part of various initiatives quickly move to the US or the European market because of better start up culture, incubation hubs and better approach to market incentives in those markets.

The Australian Government can do more to encourage innovation and assist the development of the product ecosystem by adopting one or more of the following strategies:

- Establish additional incubation and acceleration centres for start-ups;
- Encourage the start-up and commercialisation culture in academia and provide pathways for commercialisation through the incubation centres;
- Encourage and embrace domestic industry strategies for cyber security products and support them in their journey via a partnership with government both at the local and federal level; and
- Establish risk-based standards for products and services.

The Australian government has recently committed $15 billion to establish a National Reconstruction Fund.[21] A major area of the fund is science, technology and innovation which is seeing a demand for growth across the industry and economy.

There is an opportunity for the fund to invest in Australian cyber security which is an important sector for the growth and protection of the Australian economy. As cyber threats have become more sophisticated, frequent, and damaging, posing a significant risk to national security, critical infrastructure and economic stability.

RECOMMENDATION 17

KPMG suggests the National Reconstruction Fund could be expanded (or something similar be established) to include investment in cyber security. Substantive and ongoing investment will help grow a sovereign cyber capability, strengthen Australia against cyber-attacks, enhance resilience and ensure the continuity of services.

17. How should we approach future proofing for cyber security technologies out to 2030?

Futureproofing cyber security

Governments across the globe need to make clear the expectation that technology is designed with security in mind. Australia can, and should only have to, do so much to shift global technology practices. Secure-by-design and deployment should be a priority for Australia's international advocacy efforts. Legislative and common law mechanisms should be considered to hold technology developers to account for the security and safety of products and services.

The increased need for cyber security proofing as technology rapidly evolves also requires a major shift in the way awareness and cyber security culture are viewed and conducted. Implementing strong cyber security awareness and culture is essential in today's digital world. Organisations and businesses have the responsibility of handling sensitive information and the mismanagement of this will lead to potential threat events. The increase and development of adequate cyber security culture and awareness to upkeep with future threat

[21] https://www.industry.gov.au/news/national-reconstruction-fund-diversifying-and-transforming-australias-industry-and-economy

trends will decrease the chance for insider threats and external attackers.

Understanding and keeping up to date with future trends is vital in preparing for threats before the threat event occur. In today's digital world, it is crucial to be ahead of the technology and ensure that businesses and organisations are safeguarded against upcoming threats. In doing so, research on future technologies should be ongoing. The research on technology by industry and universities should be closely followed to understand where the future of cyber security may lead. Government should encourage academic and industry-led research of the long-term cybersecurity impacts of emerging and disruptive trends and technologies to stay ahead of the curve. To achieve this, a research centre should be established in partnership with one or more academic institutions and key industry groups to conduct this research on an ongoing basis. The outputs of this research should be used to inform Australian Government cyber policy, standards, and strategy.

Future-proofing cyber security technologies requires the use of advanced tools to combat risks and threats. The use of powerful tools to predict, detect, mitigate, and eliminate risks and threats within an automated process can ensure more effective protection. The use of automated tools for testing cyber security provides valuable insight and helps to mitigate risks before they can cause significant damage. As technology continues to evolve, we can expect to see even more innovative applications of digital twins and similar technology in the field of security.

Cyber experts have been warning about the threat posed by AI powered malware and ransomware, which would make attacks significantly harder to detect and contain. Guembe et al.[22] note that current commonly used methods to detect cyberattacks will not be sufficient for more sophisticated AI-based attacks due to the increased speed and complexity of such attacks. The use of AI technology should therefore additionally be encouraged for cyber defence to improve resource management and protection effectiveness. Advance automation should apply for:

- Threat detection
- Incident response
- Vulnerability management
- Compliance management
- Threat intelligence
- Updates and patching

In addition to addressing the current cyber skills shortage, ensuring dedicated cyber education outcomes as part of existing STEM pathways as described above can also work to foster ongoing innovation in Australia's cyber industry. Working with the education sector and the broader industry to establish cyber as an attractive career path and expanding the Cyber Security Skills Partnership Innovation Fund to further ensure the continuous development of cyber skills and innovation in Australia's cyber industry will work to maintain a healthy and innovative domestic cyber industry. Australia should additionally establish partnerships countries with a robust and mature cyber posture and industry, such as the United States, Estonia, and Singapore, to facilitate knowledge and skills sharing, and allowing Australia and partner countries to draw on the unique strengths the other provides.

RECOMMENDATION 18

KPMG recommend that the government encourage and incentivise industry and academia towards investment in research and development, ahead or in line with the curve of emerging technology. This should be led by a federal government agency or government sponsored industry partner that can facilitate trusted and meaningful information sharing. International advocacy and domestic legal accountabilities should be pursued as a priority to drive secure by design and deployment.

18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?

KPMG considers that the Australian Government could use procurement as a lever to better support and develop the Australian cyber security ecosystem.

Currently the government uses procurement to help meet policies objectives through Procurement Connected Policies. The Australian Industry Participation (AIP) National Framework applies to major Commonwealth Government procurements ($20 million and more). Successful tenderers for certain

[22] The Emerging Threat of Ai-driven Cyber Attacks: A Review (tandfonline.com)

Commonwealth procurements are required to prepare and implement an AIP Plan.

In our experience, the AIP National Framework could be better targeted to ensure that Commonwealth procurement helps grow the Australian economy and strengthens our domestic cyber industry and manufacturing capability. We look forward to working with the government as it progresses its Buy Australia Plan in the coming months.[23]

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

KPMG welcomes greater security standards and transparency on the security features of technology products. KPMG undertakes thorough risk assessments to ascertain product security and suitability. However, we recognise other business or individuals may not be able to undertake rigorous assessments. Improving the security standards of technology products, coupled with changing user behaviour, should help to reduce instances of cybercrime. These standards and user behaviour need to keep up with evolving technologies and abilities of cyber criminals. Indeed, KPMG's Global Tech Report for 2022 noted that while 99 percent of executives have generated returns from digital investments, 58 percent of cybersecurity teams admit that they are behind schedule due to the rapid pace of digital transformation and digitalisation seen over past several years.[24]

In addition to security standards, greater transparency on consumer data collected or generated by use of technology products, including where and when data is stored, processed and used should be available to consumers.

Security design principles or standards adopted by the Australian Government should provide clarity to technology product designers on what the minimum standards are for technology products sold in Australia.

A labelling scheme that helps consumers to make informed choices and drive improvements in product design, such as a star rating or a safety rating similar to ANCAP rating could be beneficial. Educating consumers about such ratings will be crucial to its success. Any such rating or certification system should draw from existing standards, such as the NIST Cyber Security Framework, ISO27001, and the ACSC Essential Eight. This system should be revised periodically to reflect changes to the standards that it draws from, as well as any new security standards that may be specific to certain types of emerging technology. In addition, the ACSC should work with industry experts to develop and continuously update basic security standards, akin to the Essential Eight, for key emerging and disruptive technologies to establish a baseline level of security.

Unfortunately, however, there is no silver bullet to prevent the attacks that originate due to these emerging technologies. The Strategy, therefore, should be positioned to evolve rapidly with the risk landscape and not play catch-up with technology.

RECOMMENDATION 19

KPMG supports a minimum baseline requirement for IoT, and ICS devices used in smart homes and smart cities that balances security and consumer experience. Immediate and significant investment should be made in the development of standards, appropriate use guidelines for the use of emerging technologies such as Quantum computing, Artificial Intelligence and web 3 (block chain, Metaverse) to manage potential harm to the society. A market mechanism could be considered to make quicker progress in standards development and implementation.

20. How should government measure its impact in uplifting national cyber resilience?

The Australian Government should look to numerous methods of measurement if they are to accurately assess and continually uplift the nation's cyber posture. Modelling should also be undertaken to assess if regulatory reforms are likely to create the social and economic benefits sought, in consideration of implementation costs worn by government, taxpayers, businesses and consumers, and costs of government incentives. Reviews of the reforms should be built into the legislation to ensure the reforms remain effective.

Whilst it should be considered that some aspects of cyber security are difficult to measure, there are a number of metrics which could be utilised by the government to measure the success of this national uplift, including:

- Number of significant data breaches per year;
- Number of significant cyberattacks per year;
- Number of APT events per year;

[23] Buy Australian Plan | Department of Finance

[24] KPMG global tech report 2022

- Number of citizens affected by cyber-related breaches per year;
- Number of IDCare claims per year;
- Number of cyber insurance claims settled per year;
- Number of significant cyber-attacks mitigated per year;
- Number of false flags per year;
- Number of arrests/prosecutions for cybercrime related offences per year;
- Number of successful offensive campaigns completed by ASD/AFP/ACSC;
- Estimated days taken to sufficiently recover from significant breach/attack;
- Estimated business costs associated with breaches;
- Estimated gaps in cyber security workforce; and/or
- Number of new cyber security professionals per year/number of new cyber security graduates.

Some of these metrics rely on voluntary reporting measures or biased industry reporting, so action should also be taken to ensure those metrics which are calculated are objective and accurate. Furthermore, trend analysis and annual reviews of these metrics should be enforced to allow decision makers the ability to pinpoint areas of growth, areas of concern and areas for immediate improvement/focus.

RECOMMENDATION 20

To measure the effectiveness of national cyber readiness it is important to note the required outcome prior to metrics being selected. KPMG has suggested a range of metrics that could be utilised by government to measure the success of a cyber security uplift in response to Question 20.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

Ensuring ongoing public transparency and input into the Strategy is critical to ensure its success, and to ensure public trust in Australia's cyber security infrastructure. To ensure public transparency and input, several measures can be implemented with the strategy.

Primarily, the data used to support the strategy should be made publicly available where possible, and the strategy should be subject to reviews on a periodic basis. As part of these periodic reviews, an independent evaluation of the effectiveness of the Strategy should be conducted, with the results of this evaluation shared with the public and news media.

To ensure the public has an input into the strategy, a feedback loop should be established that emphasises communication with stakeholders in small and medium enterprises, the cyber industry, large organisations, academia, the public, and government. This feedback can be gained by hosting focus groups on the strategy with representation from each stakeholder group, including the general public, as well as gaining a broader picture of public perceptions and feedback on the Strategy by conducting online surveys relating to the Strategy, with the inclusion of questions to gauge how engaged respondents are with the Strategy, how effective respondents believe the strategy is, and potential areas for the Strategy to improve. Any such surveys should be effectively advertised on news and social media to ensure that its reach is as broad as possible.

RECOMMENDATION 21

To support ongoing public transparency and input regarding the implementation of the strategy KPMG recommend that a feedback loop be created and implemented. This should include focus groups with general public and cyber security subject matter experts and short surveys to key enablers of the strategy.

Key authors and contacts

Martijn Verbree
Lead Partner, Cyber Security

Greg Miller
Lead Partner, Government Cyber and Critical Infrastructure

Mark Tims
Partner, Technology Risk & Cyber

Gergana Winzer
Partner, Cyber Lead – Mid Market

Veronica Scott
Partner, Cyber, Privacy & Data Lead, KPMG Law

Kelly Henney
Partner, Privacy & Data Protection Lead

Carlo Cappuccio
Director, Management Consulting

Stefanie Cordina
Director, Management Consulting

Naveen Venugopal
Associate Director, Management Consulting

Benjamin Jones
Associate Director, Management Consulting

Merriden Varrall
Director, Geopolitics Hub

Jon Berry
Associate Director, Geopolitics Hub

Simran Grewal
Senior Consultant, Management Consulting

Andrew Sneddon
Consultant, Government Cyber, Management Consulting

Kenneth Watkins
Consultant, Cyber, Management Consulting

Sophie Finemore
Director, Corporate Affairs

Olivia Spurio
Manager, Corporate Affairs

KPMG.com.au