AustCyber
Part of the Stone & Chalk Group

28 April 2023

Expert Advisory Board
Department of Home Affairs
Email: auscyberstrategy@homeaffairs.gov.au

Re: AustCyber submission to 2023-2030 Cyber Security Strategy Discussion Paper

Thank you for providing us with an opportunity to make a submission on the Australian Government's consultation for the 2023-2030 Cyber Security Strategy (Strategy) Discussion Paper.

This is a timely consultation, and we welcome the appointment of the Expert Advisory Board to provide strategic advice to the Minister for Home Affairs and Cyber Security, and who will be working with the Department of Home Affairs (Home Affairs) to develop this Strategy.

1. Introduction

1.1 About Stone & Chalk Group

As a representative of Australia's large innovation community, our mission at the Stone & Chalk Group is to transform Australia into a sustainable tech-driven economy.

There are opportunities presented by emerging technologies and it will be important to ensure that we have a sustainable local technology industry in Australia. With a strong innovation ecosystem, this will in turn lead to more job opportunities and enable Australian businesses to become more globally competitive in the long term. This can be realistically achieved if we have an entrepreneurial pathway for accelerators and a more curated innovation ecosystem.

To support this, we need to have access to a sustainable pipeline of talent and skills to meet the demands of the emerging high-tech industries. We also need to ensure that we are a globally competitive environment for investment into the research community, as well as in startups and scaleups, from their early research and development phases through to commercialisation.

As part of this framework, Stone & Chalk Group has played a catalytic role in enabling the growth of startups and scaleups across Australia. Our initial focus began in fintech, where we helped facilitate the growth of that ecosystem, seeing the emergence of iconic fintech players.

More recently, we have been growing a more holistic emerging technology ecosystem including cyber security, web3, artificial intelligence, quantum, proptech, climate-tech, medtech, agtech, and other scaling businesses with novel products and global ambitions.[1]

1.2 About AustCyber

As part of this growth, AustCyber merged with Stone & Chalk Group in February 2021, consistent with the previous Australian Government's request for Industry Growth Centres to establish a pathway to be financially sustainable. This merger affirms our confidence in the next phase of the evolution of the Australian cyber security sector. Since that time, AustCyber continues to undertake important initiatives to help grow the sector in Australia.

At AustCyber, we remain committed to continuing our ongoing support of the cyber security needs of all, including startups, scaleups, corporations and government, through our AustCyber Australian Cyber Security Innovation Centres across the country.

To help Australia become a sustainable tech driven economy, AustCyber plays a key role in encouraging people and businesses to protect themselves from cyber threats, ensuring our young cyber security sector receives the necessary support to enable it to grow competitively.

1.3 AustCyber 2022 Sector Competitiveness Plan

In November 2022, as part of our Australian Cyber Week, we released AustCyber's flagship publication, the 2022 Sector Competitiveness Plan (SCP).[2] The SCP is designed to help shape, inform, and grow Australia's vibrant and globally competitive cyber security sector.

[1] Further information about Stone & Chalk can be found here: https://www.stoneandchalk.com.au/resources/.

[2] A copy of our SCP can be found here: https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2022.

AustCyber
Part of the Stone & Chalk Group

In the most pressing time of our cyber security history, with cyber security becoming an increasing national concern, it is a critical and opportune time to share knowledge and insights that identify risks and opportunities, deliver proposed solutions, and encourage healthy national debate on our cyber security industry.

The 2022 SCP provides key findings around three critical themes that are fundamental to the sustainability of the cyber security industry in Australia, and present significant economic value in terms of growth, exports, and education. Building on our findings, we also heard during Australian Cyber Week from leading experts who shared their insights around these subjects.

Since the release of the SCP, we have seen major government announcements made to strengthen our cyber security capabilities globally. That being said, we are still witnessing fundamental concerns that need to be addressed with urgency and priority, if we want Australia to gain a reputation of being the most secure nation by 2030, or indeed be more ambitious to become a global cyber security superpower. AustCyber's vision for Australia is that it should strive to become a top five global cyber security leader and sustain this. With the Brisbane Olympics being held in 2032, it would be a significant win if Australia could achieve this top five ranking by then and celebrate this success as we do when we succeed in sports.

For the purpose of this submission, our comments are largely drawn from the 2022 SCP, addressing the questions raised in the Discussion Paper. We would also welcome the opportunity to work closely with the Advisory Expert Panel, Home Affairs, and other key government agencies and stakeholders as it develops the Strategy.

1.4 Summary of recommendations

Below is a summary of our recommendations in response to the questions. We grouped the questions based on common themes that arose while answering them, namely: cyber security vision for Australia; legislations, regulations, and standards; ransomware measures; international partnerships and trade; information sharing; talent; industry and research investment; and future industry.

AustCyber
Part of the Stone & Chalk Group

Section	Discussion Paper Question No.	Recommendations

Section 2. Cyber security vision for Australia	1, 20, 21	• Australia should aim to be a top five cyber secure and competitive nation in the National Cyber Security Index by 2030.
		• Australia should aim to add $800 million to annual cyber security revenue by 2026, which can be achieved by addressing the following three key areas:
		  ○ Support research, innovation, and startup development;
		  ○ Bolster domestic procurement and export capability; and
		  ○ Attract local and international talent.
		• AustCyber has contributed to the Government's Cyber Security Strategy thanks to support from government and industry stakeholders. Some programs will require ongoing support and we welcome working through these activities with our key stakeholders.
		• To maintain Australia's position on the forefront of cyber security innovation and industry development and contribute to the Government's 2030 vision, it is recommended that investment to grow the cyber security sector in Australia is adequately funded in the longer term. AustCyber can help deliver this objective, along with support from key industry and government stakeholders. It is imperative that government and industry stakeholders continue to support the momentum of AustCyber's work through adequate funding.
		• More broadly, our submission covers several areas that can help contribute to the Government's Strategy. We welcome collaborating with the government and other stakeholders to help co-design an effective Strategy with

Section	Discussion Paper Question No.	Recommendations
		measurable outcomes to deliver on the Government's vision.
Section 3. Legislations, regulations, and standards	2a, 2b, 2c, 2d, 2e, 6, 13a	• We would welcome working with government and key stakeholders to ensure a more regulatory coherent approach towards cyber security best practices via standards across Australian government agencies and jurisdictions and extended further through international standards setting bodies. • Any proposed amendments to the Security of Critical Infrastructure Act should be subject to proper cost-benefit analysis, especially its impact on smaller businesses. Proportionate cyber security uplift support should also be offered to businesses that are captured by any reforms. • Beyond regulatory responses, ongoing education and training plays a critical component to uplifting the cyber security posture of businesses. Ongoing government support in this domain will therefore be important. • If the government decides to proceed with a Cyber Security Act, we would welcome understanding further its scope and objective. Productive purposes of a new Act could include reducing regulatory duplication of existing cyber security requirements, improving coordination between government agencies and regulations, clarifying shared responsibilities/obligations between governments and entities, and promoting domestic procurement and investment in cyber security products and services. • There would be benefit in exploring the option of a single body that can coordinate between the interrelated areas of cyber security, online safety, and online privacy.
Section 4.	2f, 2g	• We strongly support the Government's ongoing, joint standing operation between the AFP and ASD to tackle

AustCyber
Part of the Stone & Chalk Group

Section	Discussion Paper Question No.	Recommendations
Ransomware measures		ransomware threat groups, and the Government's role in chairing the International Counter Ransomware Task Force to drive international cooperation to tackle ransomware. • We would welcome helping to sharpen this further, working with government and industry to support businesses to help them uplift their cyber posture.
Section 5. International partnerships and trade	3, 4, 5	• We would strongly welcome government support for our partnerships with Austrade, and other State and Territory government agencies, to help boost the export capability of our Australian cyber security businesses. • Further government investment should be given to the following areas: ○ Collaboration and coordination between the various Australian government jurisdictions and agencies and industry stakeholders on global trade support activities to raise awareness of how we can collectively assist companies to export. This covers our different regions of government and areas of government focused on cyber security. ○ Promote better the success stories of domestic cyber security businesses that have been able to export and unpack how they have done so well, and lessons that their peers could learn from those journeys (warts and all). ○ Industry and government working closely on how to support and deliver successful trade delegations and missions around the globe for cyber security. ○ Further explorations about the implications of free trade agreements and other alliances between Australia and other countries that strengthen our trade ties that could flow onto our cyber security businesses (e.g.,

Section	Discussion Paper Question No.	Recommendations
		AUKUS trilateral partnership, various free trade agreements, and other global security partnerships such as the Quadrilateral Security Dialogue, Five Eyes Alliance, and other friendly countries including EU and Indo-Pacific regions). As similar matters have been raised in the recently released Defence Strategic Review, there is an opportunity to align these discussions with the Cyber Security Strategy Review. ○ Explore integrating government trade support with domestic government procurement to strengthen government promotion of exports. This should provide a demonstrated form of assurance by the Government for the companies that they are seeking to promote (subject to appropriate probity and procurement rules).
Section 6. Information sharing	7, 8, 9	• We welcome exploring ways to improve information sharing regarding cyber security incidents between governments and industry. In addition to exploring safeguards for information providers, other potential barriers (if any) should be further investigated. • Raising public awareness regarding cyber security threats, akin to a public campaign similar to "Slip, Slop, Slap, Seek and Slide" for cyber security and safety would be worth exploring further.
Section 7. Talent	11, 12	• Our education system requires ongoing reform to ensure it develops a longer term pipeline of talent, and responsive to the continually evolving emerging tech environment. This should start early at schools and be co-designed in partnership between schools, industry, and governments to build effective school programs around

AustCyber
Part of the Stone & Chalk Group

Section	Discussion Paper Question No.	Recommendations
		entrepreneurship, innovation, and cyber security and cyber safety. This could entail prioritising appropriate government funding of industry-school partnerships in these domains. • In collaboration with key stakeholders, Australian cyber security leaders have joined forces with us to create the Australian Cyber Security Professionalisation Program (ACSP) to build sustainable career pathways for industry professionals. As this is progressing through its development stage, ongoing government and industry support for this initiative is critical to enable advancement to the next important phase to continue this great work. • Processing of applications for skilled tech workers under the permanent Skilled Nominated visa and short-term Temporary Skills Shortage visa should be benchmarked against our international peers. • Processing of critical visa applications should be extended to cyber security talent, as well as professionals ranging from ICT specialists to analyst programmers and software engineers. • Additional measures to address the backlog of skilled worker visa applications should be explored such as increasing funding support for accelerating the processing of applications and reducing wait times. This may be in the form of recruiting more public service workers and procuring technologies that will expedite the processing of applications. • A specific attraction campaign should be conducted specifically targeting cyber security and other high tech specialist talent overseas in order to increase the quantity and quality of applicants in Australia. • Appropriate government funding should be allocated to bridge diversity and inclusion initiatives that enable access to talent with building innovation ecosystems and cyber security capabilities across Australia.

AustCyber
Part of the Stone & Chalk Group

Section	Discussion Paper Question No.	Recommendations
		Attached to funding should be clear measures of success and a vision of where we want to be in the short to long term horizon.
Section 8. Industry and research investment	15a, 16, 18	• We would welcome ongoing support from government and industry to help support the cyber security uplift for smaller businesses. • Government investment in the cyber security sector has been critical to date. Given the industry's infancy in Australia compared to other more established sectors, it is important that the cyber security sector (especially startups and scaleups) receive ongoing support in growing their businesses. • Early-stage funding in Australian cyber security startups and scaleups should be increased to improve their international competitiveness, supported by access to a larger venture capital market and government investment. • To promote the growth of promising Australian cyber security startups and scaleups, it is recommended that additional project funds are allocated for business growth and cyber security accelerator programs. • As the Future Made in Australia Office establishes itself, we look forward to working with the Government to ensure that procurement of solutions from startups and scaleups, especially in the cyber security industry, are properly supported to succeed and help the Government achieve its procurement policy objectives. • We would welcome further investigation into how the challenges of domestic security responses to cyber security and national security (e.g., amended SOCI Act and Privacy Act, and the recently announced Defence Strategic Review that specifically calls out cyber security as a critical domain) can be turned into a positive

Section	Discussion Paper Question No.	Recommendations
		opportunity to create a competitive advantage for our domestic cyber security capability that can be converted into our global comparative strength. • R&D government funding support for cyber security should be increased to be more comparable with other emerging tech investments such as AI in the Australian Research Council (ARC). However, caution needs to be given against prioritising between emerging technology investments**.** This can be achieved by augmenting R&D funding through ARC grants and by enhancing the scope and transparency of R&D tax incentives, both of which will contribute to the advancement of cyber security research and industry development. • The Government can foster a more robust innovation ecosystem by persisting in collaborating across key stakeholders and by promoting the growth of innovation hubs. It would be beneficial to establish metropolitan and regional cyber security innovation hubs, which can help to encourage innovation, build cyber security communities, and offer a collaborative platform to all key stakeholders in the sector. These stakeholders may include federal and state governments, corporates, international and local cyber security companies, law enforcement agencies, industry bodies, academic institutions, and the general public. In this regard, through the Federal Government's support, AustCyber is establishing its national network of AustCyber Australian Cyber Security Innovation Centres and we would welcome collaborating with stakeholders to provide a meaningful impact as these are rolled out.[3]

[3] See https://www.austcyber.com/national-node-network for further information.

AustCyber
Part of the Stone & Chalk Group

Section	Discussion Paper Question No.	Recommendations
		• Appreciating the challenge of supporting various emerging tech initiatives including in R&D, we would welcome working with Government and key stakeholders to tackle this, for example, through the development of a national industry development and/or innovation strategy. • A workshop (or a series of workshops) should be held with key stakeholders to explore key areas where government and industry could support helping to grow our domestic industry capability in cyber security that provides meaningful and more immediate impact. These could help to unpack further matters including in relation to industry needs such as cyber security startup and scaleup support, procurement support and R&D support, as well as other areas covered in our recommendations (e.g., talent and exports support). As AustCyber is already actively engaged in supporting industry growth, we would be happy to assist the Government in this regard and coordinate with support from key stakeholders.
Section 9. Future industry	17, 19	• We would welcome working with the Government and other key stakeholders to review cyber security related issues associated with emerging tech. • Further review should be given to Australian preparedness for the cyber security implications of emerging tech such as quantum technology, AI and Web3.

AustCyber
Part of the Stone & Chalk Group

Should the Advisory Expert Panel have any questions regarding this submission, please do not hesitate in contacting our Director, Government Relations & Policy Advocacy, Charles Hoang. He can be reached directly at [redacted]

Yours sincerely

[redacted]

Michael Bromley
Chief Executive Officer
Stone & Chalk Group

AustCyber
Part of the Stone & Chalk Group

2. Cyber security vision for Australia

- ***Discussion Paper Question # 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?***

2.1 Vision

First, we should strive to become a top five cyber security nation in the National Cyber Security Index by 2030.[4] We should aim to not only be the most cyber *secure*, but also most cyber *competitive*. This implies that we are looking at proactively investing in a competitive domestic cyber security and wider industry, as well as protecting them from cyber security threats. Cyber security is not only a shared *responsibility* between governments, industry, and the wider community - it should be a shared *interest* for all.

2.2 Key areas

Our SCP highlighted several key findings that we would like to bring to the Government's attention:

- Australian cyber security startups receive 300 times less funding than international peer leaders.
- Australian cyber security firms are focused on servicing a relatively small domestic market. The Australian market represents only 2.1% of global cyber security demand.
- Government funding directed to cyber security research has also decreased from $9.8 million in 2019 to $7.5 million in 2022.

Our SCP also found that Australia has an opportunity to add $800 million to annual cyber security revenue by 2026 through three key areas:

- **Support research, innovation, and startup development**: Increase incentives and funding for R&D, as well as support the innovation ecosystem, to address the challenge of limited startup support:
    - Increase R&D funding from the Australian Research Council to match peer economies, such as Israel, the United States and Singapore. Increasing R&D funding to universities will boost innovation and creation.
    - Continue to refine and illustrate the scope and clarity of R&D tax incentives for software development to promote R&D in the sector.
    - Continue collaboration between businesses and educators and promote the development and early adoption of advanced technologies via innovation hubs.
    - Continue to mature the innovation hubs by coordinating sector engagements and aligning policies to sector needs.

[4] NCSI, https://ncsi.ega.ee/country/au/.

- **Bolster domestic procurement and export capability**: Support domestic procurement of cyber security, alongside continuing efforts to grow exports, thereby providing a broad base of growth:
    - Continue to improve government procurement systems to support procurement for domestic cyber security firms.
    - Grow the domestic cyber security market by supporting SMEs with cyber security education and cyber security implementation.
    - Maintain strong government support for the cyber security sector by supporting AustCyber's and Austrade's trade delegations. Provide market research publications, training, and introductions to customers.
    - Support entrepreneurs to visit Silicon Valley, to provide them with valuable entrepreneurial experience in the California tech hub.

- **Attract local and international talent**: Work together on attracting talent and upskilling workers to take the handbrakes off the Australian cyber security sector growth:
    - Maintain attractiveness of the sector as an employer by offering competitive wages via employee-share programs.
    - Support international talent to relocate to Australia by fast-tracking skilled visas. Skills programs are currently costly and with a long application process, limiting the pool of potential workers.
    - Develop a strong diversity and inclusion strategy to recruit a diverse and inclusive workforce, focusing on under-represented and under-served groups and regions.
    - Continue work from the National Skills Commission. Invest in future cyber security talent by partnering with educational providers through placements and work integrated experiences, research and innovation opportunities, and career opportunities.
    - Build on the success of AustCyber's education map to provide information on cyber security education. Continue supporting clear and accessible pathways to retain and upskill workers in the current workforce via VET and university offerings.

2.3 AustCyber activities supporting Cyber Security Strategy

Through the Industry Growth Centres initiative, AustCyber was established in 2017 and has played an important role in advancing the cyber security sector. It has been successfully fulfilling its commitment to foster innovation, expansion, and export in the sector through its diverse range of programs and initiatives.

Driven by the mission of growing, exporting and education, AustCyber has aided the development of a vibrant and growing network of Australian-based cyber security businesses, promoting Australia's reputation as a hub for cyber security innovation globally. Today, there are an estimated 291 businesses in the sector.

However, there is still more important work required through ongoing industry investment, especially if we want to meet the Government's challenge for Australia to be the most secure nation by 2030. And it has never been a more critical time to invest in and develop the industry to enable Australia to keep up with the latest advancements in the field of cyber security, where we are seeing a constantly evolving global cyber security threat landscape, emerging technologies, and dynamic threat landscape.

For instance, there are a range of activities that AustCyber is engaged in and working with key partners to deliver that will support the cyber security sector and the Strategy.
These include:

- Australian Cyber Security Professionalisation Program (ACSP): https://www.austcyber.com/file-download/download/public/1712
- AUCyberscape: https://aucyberscape.com/
- AUCyberExplorer: https://www.aucyberexplorer.com.au/
- Cyber Battle: https://www.austcyber.com/cyber-battle-2023
- Cyber Security Traineeship Program: https://www.megt.com.au/microsoft-traineeship-program/cyber-security-program/candidates
- AustCyber Projects Fund: https://www.austcyber.com/grow/projects-fund
- National Network of AustCyber Australian Cyber Security Innovation Centres: https://www.austcyber.com/national-node-network
- Cyber Security Ambassadors: https://www.austcyber.com/ambassadors

In addition to government support, AustCyber's activities can only be successful if they are designed and implemented collaboratively with other key stakeholders. Going forward, AustCyber plans to continue to help coordinate and work closely with like-minded stakeholders to support cyber security sector growth in Australia.

2.4 Measures for success

- ***Discussion Paper Question #20: How should government measure its impact in uplifting national cyber resilience?***
- ***Discussion Paper Question #21: What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?***

We have addressed Questions 20 and 21 together as our responses are interrelated.

With the Government's vision for Australia to become the most secure cyber nation by 2030, it would be useful to understand the areas that will enable us to reach this position.

According to the National Cyber Security Index, we are currently ranked 40th in the world.[5] We should at least be striving to improve these rankings to reach the top five and 2030 might not be insurmountable if the proper actions are put in place to address areas that require improvement.

Our submission highlights several areas where improvement can be made which in turn can improve our rankings. We are happy to work with the Government and key stakeholders to ensure that this is achievable.

Recommendations:

- **Australia should aim to be a top five cyber secure and competitive nation in the National Cyber Security Index by 2030.**
- **Australia should aim to add $800 million to annual cyber security revenue by 2026, which can be achieved by addressing the following three key areas:**
    - **Support research, innovation, and startup development;**
    - **Bolster domestic procurement and export capability; and**
    - **Attract local and international talent.**
- **AustCyber has contributed to the Government's Cyber Security Strategy thanks to support from government and industry stakeholders. Some programs will require ongoing support and we welcome working through these activities with our key stakeholders.**

[5] Ibid.

- **To maintain Australia's position on the forefront of cyber security innovation and industry development and contribute to the Government's 2030 vision, it is recommended that investment to grow the cyber security sector in Australia is adequately funded in the longer term. AustCyber can help deliver this objective, along with support from key industry and government stakeholders. It is imperative that government and industry stakeholders continue to support the momentum of AustCyber's work through adequate funding.**
- **More broadly, our submission covers a number of areas that can help contribute to the Government's Strategy. We welcome collaborating with the government and other stakeholders to help co-design an effective Strategy with measurable outcomes to deliver on the Government's vision.**

AustCyber
Part of the Stone & Chalk Group

3. Legislations, regulations, and standards

We have addressed Questions 2a and 6 together as our responses are interrelated.

3.1 Standards

- ***Discussion Paper Question #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)?
- ***Discussion Paper Question #6: How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?***

Harmonising standards is a crucial area of focus for streamlining the challenge of understanding a baseline of best practice for cyber security. Cyber security professionals will have their preferred standards. Nevertheless, organisations must consider their unique context and risk appetite. If implemented effectively, standards drive improvement to organisational cyber security.

For example, ISO/IEC 27001 is a recognised international standard for cyber and information security. However, it is not uncommon for there to be other standards that are referenced by governments and industry across sectors and jurisdictions.

As cyber security is a global challenge, we should be influencing it both domestically and internationally. This can be achieved through ISO and other international standards organisations that already exist to address historical challenges like safety. In addition, this will need to encompass accreditation and certification organisations, comprising skilled professionals who are not yet fully equipped to respond to the cyber security challenge.

National, State/Territory, and sector-based regulators should recognise existing standards and only seek to augment them where necessary. Although the APRA CPS 234, the Defence Industry Security Program (DISP) and Security of Critical Infrastructure Act reforms go to some extent in addressing multiple cyber security requirements, there is more room for regulatory coherence.

For example, sector-based schemes can be developed to augment ISO/IEC 27001. Moreover, a baseline standard like ISO/IEC 27001 may need to be augmented by more technical standards in certain areas like software development, IoT, and AI/ML, which should be encouraged.

More importantly, the Government needs to harmonise fraud controls that require retention of identity documents with privacy laws that seek to minimise storage of sensitive personal information. Digital ID can be an effective mechanism to address this.

Of course, there is also a question of proportionality. While ISO/IEC 27001 is the most practical and extensible cyber security standard, it may remain a challenge for small businesses. Another recognised Australian cyber security framework is the ASD Essential Eight - it is often referred to by Australian government agencies and larger entities. However, it is known in the market that it is harder to implement by smaller businesses - making it more accessible for these businesses to implement would be an important starting point, especially if they are referred to in procurement processes. Therefore, small businesses will instead need to rely on their supply chain and secure defaults, or otherwise receive appropriate cyber security uplift support.

As an incentive, government procurement processes can help drive cyber security standard compliance. However, the challenge is where there may be different procurement processes that refer to different standards as proxies for cyber security best practice. We would welcome working with government and other key stakeholders to ensure a more coherent regulatory approach towards cyber security best practices across government agencies and jurisdictions. This could extend further into discussions regarding internationally coherent approaches via international standards (discussed further below in response to Question 5).

For example, in partnership with the NSW Government, AustCyber and Standards Australia facilitated the NSW Standards Harmonisation Taskforce (comprising industry representatives and experts), releasing a cyber security standards recommendations report in February 2021.[6] High level insights from the report included:

- There is a myriad of cyber security standards to select from. Some standards (i.e., ISO, IEC, EN, NIST) are embedded into policy and assurance frameworks and others are not.

[6] NSW Government, 'Release of cyber standards recommendation report' (News release, Feb 2021), https://www.nsw.gov.au/news/release-of-cyber-standards-recommendation-report.

- Good practice will differ between sectors, in relation to entity size, threat surface, risk appetite, maturity and customer orientation.
- Care must be taken to factor-in how standards are to be used, for what purposes and in relation to specific public policy requirements. This might include consideration of the relative merits of principles-based approaches, attestation, certification and how development, adoption or use of standards might impact supply chains or procurement behaviour.
- The quality and volume of guidance material on implementation of specific standards needs to improve. This includes how the material maps to government frameworks (existing or proposed).
- A cyber security workforce skills gap exists in relation to understanding and application of standards and compliance.
- Some targeted government support might be required for specific growth sectors (i.e., to support market entry in more complex markets and where there might be a significant return on investment).

3.2 Security of Critical Infrastructure Act

- ***Discussion Paper Question #2b: 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?***

The Security of Critical Infrastructure (SOCI) Act was amended in December 2021 and April 2022, which saw a wider range of sectors and entities subject to new security obligations, including cyber security. This also potentially extends to smaller businesses including those along the supply chain.

With many organisations relying on third party providers, supply chain security has remained an issue. In practice, organisations that are susceptible to supply chain security breaches fail to recognise the breadth of their supply chain risk and defend themselves against such incidents. This is even though there indeed exist standards that address supply chain security.

In light of the effects of the pandemic, geopolitical tensions and supply chain disruptions, there has been a global trend towards sovereign capability development. Standards and supplier chain credentialing through third party audits against standards will aid in the dispersion of appropriate technologies.

There is a role for the Government in procuring proven Australian cyber security products and services. The government can also subsidise the cost of third-party audits to encourage providers to increase organisational and supply chain security.

More recently the Government's Office of Impact Analysis estimated that the cost of complying with the critical infrastructure risk management program rules' one-off aggregated national cost to be around $1.6 billion, with an ongoing aggregated cost of around $1.08 billion per year. This is an overall regulatory cost of $11.5 billion over a decade.[7] How the regulatory costs translate and pass down to smaller less established businesses along the supply chain is unclear.

Regarding further amendments to the SOCI Act, it is important to recognise the deeper impacts that any further amendments might have on smaller businesses. Therefore, extending definitions that might capture more businesses, operations and data will need proper cost-benefit analysis and cyber security uplift support for businesses.

3.3 Company directors' obligations

- ***Discussion Paper Question #2c: Should the obligations of company directors specifically address cyber security risks and consequences?***

In terms of legal obligations for company directors, we note that recent case law exists that provides some guidance in this domain. In particular, there were two recent Australian cases, *ASIC v RI Advice Group* [2022] FCA 496 and *DRB Group v Canberra Hydraulic Engineering Services* [2022] ACAT 30, that set a precedent around cyber security related governance obligations for boards and directors.[8]

We are also all aware of the growing public expectations and government regulatory responses to recent major cyber security incidents and data breaches. This has included amendments to the Privacy Act with increasing penalties of up to $50m for privacy breaches, in addition to the 2021 & 2022 amendments to the SOCI Act. The Attorney-General's Department has also released its final report on the Privacy Act Review, making recommendations that should be also considered in this Cyber Security Strategy Review.

---

[7] 'New critical infrastructure obligations to cost $1bn annually' (InnovationAUS article, Feb 2023), https://www.innovationaus.com/new-critical-infrastructure-obligations-to-cost-1bn-annually/.

[8] 'First Australian court judgments on cyber security' (AICD article, Jun 2022), https://www.aicd.com.au/economic-news/world/global-risk-report/first-australian-court-judgments-on-cyber-security.html.

A natural (somewhat blunt and simplified) response has been to increase penalties and fines for data and cyber security breaches. It is hoped that this will incentivise businesses to uplift their cyber and data security posture and create a real shift in Board discussions to reconsider the value and criticality of cyber security. However, penalties, compliance measures and other responses are only tools.

At the Board level, cyber security and technology literacy has been discussed more generally for a while now. According to a 2022 Proofpoint and MIT Sloan report:[9]

> "Of the 600 board members across 12 countries surveyed globally, key Australian findings reveal: … Only 58% of Australian board members see cybersecurity as a top priority – the least of all 12 countries surveyed (global average 77%)."

Risk mitigation is a tough sell. An early-stage startup for example will spend time building new features in its search for product/market fit, however the businesses are so focused on earnings and market success, it can be tough for them to understand the criticality of investing in important areas that do not directly contribute to increased revenue, such as preventative security. The same applies for more established companies.

It is becoming more and more evident how critical it is for businesses and Boards (regardless of size and maturity) to prioritise analysing their risk around the economics of potential security breaches, and very importantly plan accordingly.

Boards must start thinking of cyber security as an enabler for businesses rather than a cost centre. Cyber security is about managing risks and ensuring business continuity that in turn generates revenue.

Good cyber security and associated measures are only as strong as the culture and leadership that is driving it - it starts from the top, which should then permeate down to others throughout the business.

To address this, beyond regulatory responses, we firmly believe that ongoing education and training plays a critical component to uplifting the cyber security posture of businesses. Ongoing government support in this domain will therefore be important.

---

[9] 'Australian Board Members Lagging in Cybersecurity Maturity' (Australian Cyber Security Magazine article, Oct 2022), https://australiancybersecuritymagazine.com.au/australian-board-members-lagging-in-cybersecurity-maturity/.

AustCyber
Part of the Stone & Chalk Group

3.4 Proposed Cyber Security Act

- ***Discussion Paper Question #2d: Should Australia consider a Cyber Security Act, and what should this include?***

The Strategy consultation presents a timely opportunity to undertake a proper stocktake of the current state of privacy and cyber security and safety posture, and maturity in Australia across a range of areas. This includes reviewing our current incentive and regulatory regimes, as well as barriers that may inhibit our cyber security and privacy posture and maturity e.g., access to talent, industry capability and investment.

Regarding a proposed Cyber Security Act and what this might cover, we need to be clear on whether we have properly identified the problem (e.g., understand the causes, drivers, barriers, and objectives) before we leap into a solution(s) (e.g., legislative, regulatory, or non-regulatory response(s)).

We certainly support a regulatory framework that is fit-for-purpose to reflect the modern environment. We would be cautious against inadvertently creating regulation that is another "cost for doing business" in Australia and a compliance-mindset versus a best practice mindset. These would be suboptimal outcomes and not conducive to industry development and growth in Australia.

As noted above, the Attorney-General's Department's final report on the Privacy Act Review, includes several recommendations (not limited to Chapter 21 of the final report) that could be relevant in the context of a proposed Cyber Security Act and other cyber security related measures. Ideally, any reforms that are implemented from the Privacy Act Review should be streamlined with the Cyber Security Strategy Review to minimise regulatory duplication. For example, there will likely be an overlap when having regard to: subjects about personal information, data protections, data breaches, data stewardship and information security; whether or not these should be regulated further; how they should be regulated; organisational obligations; and who should regulate them.

If a Cyber Security Act were to be considered, it would also need to have regard to its objectives and scope with respect to other legislative and regulatory obligations. At a minimum, it will need to avoid duplicating existing requirements such as under the SOCI Act, which includes a range of cyber security measures and obligations for targeted entities. This should also ensure that there is acknowledgement that cyber security is a shared responsibility that is not limited to industry and other entities and extends to governments.

On another point, regulation can drive industry growth as seen overseas. According to the SCP, the annual revenue growth of the Australian cyber security sector has averaged 8.7% over the past five years, significantly slower than other leading cyber security jurisdictions that have inadvertently grown as a result of geopolitical tensions, ecosystem benefits and strict regulations. Underspending in Australia across several key areas has seen a less globally competitive cyber security sector, diminishing our domestic capability, and presenting both an economic and national security risk. However, Australia has an opportunity to add $800 million to annual cyber security revenue by 2026 and catch up with our international peers. This will require immediate focus and investment in the sector. Consideration could be given as to whether a Cyber Security Act can help to promote domestic investment and procurement in local cyber security products and services.

3.5 Addressing regulatory burden

- ***Discussion Paper Question #2e: 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?***
- ***Discussion Paper Question #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?***

We have responded to Questions 2e and 13 together as we consider that they are interrelated.

For industry, there would be benefit in greater coordination and integration between various government agencies, authorities, and departments (as well as associated legislations and regulations) under a single body with respect to interrelated areas of cyber security, online safety, and online privacy. Providing better coordination between government agencies and regulations, and improved clarification of shared responsibilities/obligations between governments and entities could be productive purposes for a new Cyber Security Act.

Beyond regulations, a single cyber security body empowered by legislation could also allow for a more holistic oversight of the incentive mechanisms associated with cyber security and ensure a proper balance is struck between regulations and incentives. In this regard, we look forward to working with the newly announced National Office for Cyber Security, which could play an important role here.

Recommendations:

- **We would welcome working with government and key stakeholders to ensure a more regulatory coherent approach towards cyber security best practices via standards across Australian government agencies and jurisdictions and extended further through international standards setting bodies.**
- **Any proposed amendments to the Security of Critical Infrastructure Act or creation of a new Cyber Security Act should be subject to proper cost-benefit analysis, especially its impact on smaller businesses. Proportionate cyber security uplift support should also be offered to businesses that are captured by any reforms.**
- **Beyond regulatory responses, ongoing education and training plays a critical component to uplifting the cyber security posture of businesses. Ongoing government support in this domain will therefore be important.**
- **If the government decides to proceed with a Cyber Security Act, we would welcome understanding further its scope and objective. Productive purposes of a new Act could include reducing regulatory duplication of existing cyber security requirements, improving coordination between government agencies and regulations, clarifying shared responsibilities/obligations between governments and entities, and promoting domestic procurement and investment in cyber security products and services.**
- **There would be benefit in exploring the option of a single body that can coordinate between the interrelated areas of cyber security, online safety, and online privacy.**

AustCyber
Part of the Stone & Chalk Group

4. Ransomware measures

- ***Discussion Paper Question #2f: 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?
- ***Discussion Paper Question #2g: Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?***

While we understand that some entities may be tempted to pay ransoms and extortion demands from cyber criminals if they feel they have no other option, we would discourage such actions as it would only enable cyber criminals to continue their activities against other victims. This should be akin to any other type of criminal activity.

There are underlying issues that lead victims to reaching this endpoint which requires further thought. This includes: immediate impact on the targeted victim and others of a ransomware attack (e.g., critical infrastructure that could have safety implications); preventative measures (e.g., cyber security and online safety practices to mitigate this from occurring in the first place); and responsive measures (e.g., law enforcement capabilities, and knowledge of and confidence in law enforcement support to respond to incidents if they do occur).

To this end, we strongly support the Government's announcement of an ongoing, joint standing operation between the Australian Federal Police and Australian Signals Directorate to investigate, target and disrupt cyber criminal syndicates with a priority on ransomware threat groups. We also welcome the Government's role in chairing the International Counter Ransomware Task Force to drive international cooperation to tackle ransomware.

Nevertheless, more can be done to sharpen this further through government and industry support for businesses to help them uplift their cyber posture. This will be particularly important for smaller businesses, especially emerging tech startups and scaleups, who are at the leading edge of innovation. They will need as much support as possible if Australia wants to have a globally competitive industry and economy in the future.

Recommendations:

- **We strongly support the Government's ongoing, joint standing operation between the AFP and ASD to tackle ransomware threat groups, and the Government's role in chairing the International Counter Ransomware Task Force to drive international cooperation to tackle ransomware.**
- **We would welcome helping to sharpen this further, working with government and industry to support businesses to help them uplift their cyber posture.**

AustCyber
Part of the Stone & Chalk Group

5. International partnerships and trade

- ***Discussion Paper Question #3: How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?***
- ***Discussion Paper Question #4: What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?***
- ***Discussion Paper Question #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?***

We have responded to Questions 3, 4 and 5 together as we consider that they are interrelated.

5.1 Strengthening international partnerships through improved trade

As we know, cyber security attackers do not discriminate by geographical location. It is therefore important that we work collectively together across Australia and with our overseas partners. In this regard, we welcome the Government's announcement to chair the International Counter Ransomware Task Force to drive international cooperation to tackle ransomware, including through information and intelligence exchanges, sharing best practice policy and legal authority frameworks, and collaboration between law enforcement and cyber security authorities. Government leadership in these activities are critical and we would welcome working with the Government to explore how these activities can be maximised further through translation at the industry level too.

We consider that this should also extend to international standards setting. International standards play an important role in enabling global trade and interoperability. It is important that Australia works with its overseas counterparts including in cyber security standards to ensure that we do not operate in isolation or put ourselves at a disadvantage with our global competitors.

Beyond globally coordinated cyber incident engagements, Australia also engages internationally on cyber security through various trade and other international relations activities (e.g., via Austrade and the Ambassador for Cyber Affairs and Critical Technology under DFAT).

Through our critical partnerships with several of these key government agencies, as well as trade and investment focused agencies across the jurisdictions and industry, AustCyber provides resources, incentives, and support to encourage Australian cyber security businesses to export their products and services.

Some examples include:

- Trade delegations: Australian cyber security firms, as well as related governments and academic organisations, have made 129 visits to six countries as part of our trade delegations.
- Pitching events: AustCyber has organised nine pitching events since its inception. These events involve cyber security firms pitching their ideas to governments, sector experts and academics.
- Australia's cyber security sector has increased its export revenue by $2.7 billion since AustCyber's inception in 2017.

5.2 Export challenge for cyber security sector

Leveraging on our international partnerships can help to boost the export capability of our Australian cyber security businesses.

According to the 2022 SCP on our export findings:

- Australia's cyber security sector revenue growth has been significantly slower than other leading nations because of our insufficient focus on export markets.
- Australian cyber security businesses receive a significantly smaller share of revenue from exports when compared to other international businesses. The Australian cyber security sector receives approximately 17% of its revenue from exports currently, less than half of the UK's 42% share.
- Despite cyber security products and services being well-suited to exporting (especially given the cross-border nature of cyber security threats), to date Australian businesses have not been successful in capturing this attractive global market.
- Australia accounts for only 2.1 per cent of global cyber security demand. Australia's domestic demand ranks eighth globally. The US has the greatest share of global cyber security expenditure, followed by Japan, the UK, Germany, China, France, and Canada.
- Australia's domestic demand has been gradually declining and is forecast to continue to decline. Australia's share of global cyber security expenditure is 2.1 per cent in 2022. The share is down from 2.2 per cent in 2017 and is forecast to further decline to 1.9 per cent by 2025.
- Australian cyber security firms that only focus on the domestic market have a small serviceable market. Australian cyber security firms need to expand overseas to achieve scale.

Our findings suggest that Australia is small, and a large proportion of cyber security is supplied from somewhere else in the world. Given the Australian cyber security industry is largely made up of small businesses, which includes startups and scaleups, exporting their products and services overseas is considered essential to helping grow and building these businesses to become competitive and successful.

In addition, Australian cyber security businesses that only focus on the domestic market have a small serviceable market. Focusing on serving local demand only offers very limited opportunities.

There was a collective shared sentiment during our Australian Cyber Week in November 2022 that trade is critical for Australia's success and prospects for growth which has expanded from commodities and other tangible goods to intangibles including in cyber security. Improving our trade prospects will also help build and sustain our talent pipeline and, in turn, our domestic capability.

Despite the generally understood reasons for businesses needing to export, this raises questions as to why Australian cyber security businesses are not taking advantage of the export opportunities, with less than half of them even trying to sell overseas.

Several reasons were touched upon during Cyber Week 2022 including: fear or lack of knowledge or confidence; lack of support; lack of funding; nature of service based vs products based businesses; and the tyrannies of distance and relationships from our global trading partners. So, while there may be accelerated digital transformations and expected corresponding cyber security investment, we have not seen a correlation to growth via exports.

As highlighted in the 2022 SCP, critical and immediate actions are required to overcome our export growth barriers, bolster our export capability, and give Australia an opportunity to add $800 million to annual cyber security revenue by 2026. These include supporting our domestic procurement of cyber security and maintaining and strengthening the sectors' global export-oriented outlook.

Echoing our SCP findings, Cyber Week 2022 discussions highlighted that we need to invest in continued trade outreach programs, including trade delegations, export support and study tours. These can be improved upon through increased collaboration between the various government agencies, and more strategically targeted delegations and groups.

There is certainly no reason why Australia should differ from other countries in terms of cyber security threats, and geopolitical and supply chain challenges. This leads to further questioning of domestic industrial capabilities and international trade partnerships. Australia has also seen stricter regulations introduced over the last several years associated with national security.

As raised during Cyber Week 2022, there are other opportunities through other government initiatives that should be explored further to support cyber security exports such as the AUKUS trilateral partnership, various free trade agreements, and other global security partnerships such as the Quadrilateral Security Dialogue, Five Eyes Alliance, and other friendly countries including EU and Indo-Pacific regions. Some of these international relationships have been specifically discussed in the recently released Defence Strategic Review - therefore there is an opportunity to also align these conversations.

The Australian brand in general is globally recognised as trustworthy and reliable. Many international partners would want to be associated with this brand. Awareness of this brand value and our domestic competence in cyber security may not be sufficiently clear. We should therefore aim to better align and promote our cyber security sector with that trusted Australian brand.

Further, we heard from some companies during our Australian Cyber Week 2022 that they struggled to gain traction through local government procurement and felt they had a better chance to prove themselves overseas. It was also not uncommon for some of these companies to be asked by overseas government prospects if they could demonstrate their domestic credentials with their local government as a reference.

Recommendations:

- **We would strongly welcome government support for our partnerships with Austrade, and other State and Territory government agencies to help boost the export capability of our Australian cyber security businesses.**
- **Further government investment should be given to the following areas:**
    - **Collaboration and coordination between the various Australian government jurisdictions and agencies and industry stakeholders on global trade support activities to raise awareness of how we can collectively assist companies to export. This covers our different regions of government and areas of government focused on cyber security.**

- **Promote better the success stories of domestic cyber security businesses that have been able to export and unpack how they have done so well, and lessons that their peers could learn from those journeys (warts and all).**
- **Industry and government working closely on how to support and deliver successful trade delegations and missions around the globe for cyber security.**
- **Further explorations about the implications of free trade agreements and other alliances between Australia and other countries that strengthen our trade ties that could flow onto our cyber security businesses (e.g., AUKUS trilateral partnership, various free trade agreements, and other global security partnerships such as the Quadrilateral Security Dialogue, Five Eyes Alliance, and other friendly countries including EU and Indo-Pacific regions). As similar matters have been raised in the recently released Defence Strategic Review, there is an opportunity to align these discussions with the Cyber Security Strategy Review.**
- **Explore integrating government trade support with domestic government procurement to strengthen government promotion of exports. This should provide a demonstrated form of assurance by the Government for the companies that they are seeking to promote (subject to appropriate probity and procurement rules).**

AustCyber
Part of the Stone & Chalk Group

6. Information sharing

6.1 General comment

- ***Discussion Paper Question #7: What can government do to improve information sharing with industry on cyber threats?***

It should be widely recognised that sharing threat intelligence is essential. We note that there are existing government agencies aimed at enabling information sharing with industry such as through the ACSC under the Department of Defence, and the Trusted Information Sharing Network (TISN) under the Cyber & Infrastructure Security Centre (CISC) within Home Affairs.

We have collaborated with the ACSC and CISC and welcome exploring with key stakeholders (industry and others) in how we can provide increased benefit for our community on cyber security threat information sharing.

6.2 Safeguards

- ***Discussion Paper Question #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 to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?***

The subject of information sharing and providing sufficient safeguards to protect organisations that become victims of cyber security incidents has been discussed for a while now. It highlights its continuing importance for many entities that should be sharing and reporting on incidents, while also the need for agencies to provide adequate assistance when that occurs. Providing as many assurances as possible for entities that share information will be critical to instilling trust, including protecting confidentiality, should help to alleviate barriers for entities to report to the ACSC.

In addition, it may be worthwhile exploring other barriers that might lead to entities not engaging with the ACSC. We would be happy to work with the ACSC to explore where these barriers might arise e.g., education and awareness about the role of the ACSC and value of information sharing such as how information might be used by the ACSC.

6.3 Public awareness

- ***Discussion Paper Question #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?***

6.3.1 Public awareness campaigns

A benefit of reporting cyber security incidents (as with reporting to the OAIC of notifiable data breaches (NDB) under the Privacy Act) is the development of potential insights into the trends of cyber security incidents, which can help inform policy and develop targeted solutions.

We note that the ACSC and several other government agencies (such as ACCC on online scams) provide a range of useful resources in this regard. Public awareness campaigns through various media channels are important to raise public awareness about cyber security incidents and should continue.

There is certainly room for improvement through leveraging more through trusted government partners and networks. We would welcome building further on our partnerships with government agencies in this domain to maximise the opportunities to elevate public awareness through both our cyber security and large innovation community.

We have been engaged in various activities to help raise public awareness of cyber security incidents (not limited to ransomware) for our network. This has included exploring early school age awareness of cyber security and safety solutions, as well as gauging feedback on a public campaign similar to "Slip, Slop, Slap, Seek and Slide" for cyber security and safety. We would welcome opportunities to work with governments and other key stakeholders to spread this message.

6.3.2 Organisational responsibilities

Looking beyond governments and the general public, organisations should also be encouraged to share information on security product tests and test results (subject to proper safeguards). They should be proactively working with suppliers and the open-source expert community to address root causes for cyber security vulnerabilities in their underlying software frameworks and libraries. It is crucial that common knowledge is developed to mitigate cyber security threats from happening in the first place.

AustCyber
Part of the Stone & Chalk Group

An ideal aspiration is that the focus on cyber security shifts back to secure technology over time, away from people and general awareness. While awareness is useful for problem identification and as a stop-gap measure, it is not a viable long-term solution if cyber security vulnerabilities are the result of weak technology and processes in products and services.

More investment is needed in implementing Secure-by-Design practices, securing the software development lifecycle including hardware, firmware, software applications and databases. It is important that knowledge of common weaknesses, tests and mitigations that address root causes for cyber security vulnerabilities in products and services become widespread practices. If implemented properly in partnership between industry, government and other key stakeholders, there could be an opportunity to accelerate Australia towards becoming the most cyber secure nation sooner.

Recommendations:

- **We welcome exploring ways to improve information sharing regarding cyber security incidents between governments and industry. In addition to exploring safeguards for information providers, other potential barriers (if any) should be further investigated.**
- **Raising public awareness regarding cyber security threats, akin to a public campaign similar to "Slip, Slop, Slap, Seek and Slide", would be worth exploring further.**

AustCyber
Part of the Stone & Chalk Group

7. Talent

7.1 Cyber security in schools

- ***Discussion Paper Question #11: Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?***

Part of AustCyber's mandate is to help make Australia the leading centre for cyber security education.

This starts early at school where students should be taught about cyber security and cyber safety, for example. Cyber security awareness should be second nature just like putting on a seat belt when you get in the car or brushing your teeth at night.[10] School-based programs should give schools control in how they deliver it.

One area we would like to see a stronger focus on is adding the "A (Arts)" into STEM, creating STEAM: science, technology, engineering, arts, and mathematics. Arts, design, and critical thinking are foundational skills that will have a measurable impact on Australia's future workforce and entrepreneurs. It is not just about digital and cyber literacy.

As part of these reforms, teachers are essential and will need as much assistance as possible to ensure they are properly supported (including any training required) to deploy these programs.

By way of contrast, Israel for example has almost a third of Australia's population. Despite this, Israel received almost half of total global funding in cyber security firms and received 300 times more in venture capital investment compared to Australian tech firms.[11] Part of Israel's success could be attributed to having an early head start - not only in building a globally competitive cyber security industry, but also - in talent identification at around the year six to seven mark in schools and track that talent all the way through to the workforce.

[10] 'Start educating kids about cybersecurity, says expert' (AFR article, Nov 2022), https://www.afr.com/technology/start-educating-kids-about-cybersecurity-says-expert-20221104-p5bvod.
[11] AustCyber 2022 SCP, https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2022.

Importantly, this does not mean only identifying coders. Cyber security requires a wider range of skills and backgrounds such as people skills where cyber security revolves around social behaviour, requiring insights about people and the psychology behind an attack. It is a reminder that cyber attackers are also diverse with different motives from social mischief to state sponsored attacks, with cyber hacking tools becoming easier to access via the dark web. Therefore, diversity in our cyber security talent along with more advanced cyber security technology will help to strengthen our defences against these attacks.

While Israel has national service which enables the youth to receive more training which we cannot do in Australia, Australia could adopt similar approaches that have made us globally competitive in other domains such as has been achieved in sports, where we have the Australian Institute of Sport that has produced some of our greatest global sporting talents. It would not be implausible to develop a similar approach to help hone young people's skills in the cyber security domain.

Going beyond the school system, our workforce and wider community need cyber security skills. This should not be limited to whether they decide to become a cyber security professional. Our general cyber security awareness should be akin to any form of health and safety, as well as security.

Assistance from governments and industry will be important to develop much needed cyber security education programs that provide an education pathway all the way up to the workforce.

We appreciate that there may be various cyber security and STEAM initiatives that exist to support boosting our talent pool in the longer term. Given that there are talent shortages in the immediate to longer term, compounded by the evolving nature of emerging tech, ongoing investment into our education system is critical.

We note that there are also various government consultations and other activities including the Jobs and Skills Summit consultations undertaken by the Treasury, and Startup Year Program. While these are important consultations, it is imperative that more immediate action is taken to commence implementing longer term solutions.

7.2 Cyber security workforce

- ***Discussion Paper Question #12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?***

7.2.1 General comments

In addition to education reforms around STEAM, developing a sustainable talent pipeline for Australia's cyber security workforce, this will require a multi-pronged approach. And to develop properly targeted policy solutions, this needs to be supported by relevant data.

For instance, our 2022 SCP reported that there will be 3,000 fewer cyber security workers than required by 2026. The SCP highlighted that our talent shortage dilemma is a result of projected inflows and outflows from the cyber security workforce. Although there are more people entering the sector, with enrolments and skilled migration numbers growing (albeit at a much slower rate compared to before COVID-19), this is not fast enough to keep up with attrition from the sector and increased demand.

There will be current cyber security workers who will eventually leave the workforce, including those workers retiring and others moving to other industries. Although the SCP estimated an increase in new graduates, upskilled and reskilled workers, and skilled migrants will likely replace workers leaving the workforce, projected demand for cyber security workers by 2026 is estimated to exceed supply. This issue is likely to be not limited to the cyber security sector.

For highly specialised areas such as in cyber security, Australia will need a large number of experienced workers with more than six years of deep industry expertise. These will be highly technical roles, requiring a three-year university degree, and at least another three years of on-site experience. This experience would include recognising, reacting, and managing cyber security incidents.

This expertise issue is not limited to cyber security, but also data management, software engineers and developers. Without the requisite talent, organisations will lack the appropriate capabilities to either anticipate or respond to a cyber security attack, leading to increased vulnerabilities.

This means the issue cannot be solved in the short-term labour market by adjustments or training. Addressing the problem therefore requires a two-phased approach. Firstly, skilled cyber security migrants will be required to quickly address the immediate organisational vulnerabilities. Secondly, our education system will need to be bolstered to ensure we have an ongoing pipeline of talent to draw upon to manage the continuously evolving cyber security threat landscape.

7.2.2 Training and accreditation

We are involved in two important activities with thanks to support from government and other key stakeholders:

- Australian Cyber Security Professionalisation (ACSP) Program
- Cyber Security Traineeship Program.

Australian Cyber Security Professionalisation (ACSP) Program

AustCyber, is orchestrating an industry co-design team including cyber security experts, universities, and industry associations, to create the Australian Cyber Security Professionalisation (ACSP) Program.

The ACSP represents a critical step towards professionalising Australia's cyber security industry to meet global standards while sustainably developing the local cyber security ecosystem. Once finalised, the implementation of the ACSP will help standardise and repair Australia's cyber security industry which is currently fragmented with no clear career pathway for growth and development.

The ACSP co-design team features some of Australia's leading cyber security professionals. Each member will assist in the design and development of the ACSP to ultimately build solutions that improve government, business and community trust and confidence in Australian cyber security professionals.

By establishing the role of cyber security professionals and defining career and education pathways through an accredited program, the ACSP will increase professional recognition, and bring consistency to the definition of cyber security roles in Australia. The shared understanding of critical skills, knowledge and experience that constitute a cyber security professional amongst employers and employees will ultimately result in a safer, more cyber secure business environment and an increased trust and confidence for both the employer and employee in the industry. Helping build a stronger and more resilient workforce.

Once you leave university, doctors, lawyers, and other industries with highly skilled professionals have clear steps and processes in place to evolve the skills of their workforce. Now is the time to create a similarly defined pathway for cyber security professionals in Australia, so they too can have a clear process to follow to evolve their skills and careers. The ACSP program's human-centred design and stakeholder co-design focus is a significant critical next step towards ensuring Australia has a world-leading cyber security workforce.

A significant aspect of this Program development is that it has brought together key cyber security leaders and experts to co-design it. Ongoing government support for this initiative is critical to enable advancement to the next important phase to continue this great work.

Cyber Security Traineeship Program

AustCyber has partnered with Microsoft and other leading education and training providers to offer Australians a credible alternative pathway to enter the cybersecurity industry. The Cyber Security Traineeship Program (CSTP) is designed to help aspiring cyber security professionals build a rewarding career in the sector, regardless of their age, background, or experience. It will support around 200 participants over the next two years.

The program is partly funded by the Australian Government's Cyber Security Skills Partnership Innovation Fund, which aims to improve the quality and availability of cyber security professionals across the country.

Combining formal training with paid, on-the-job experience, the two-year program will allow participants to earn while they learn. Trainees will spend four days a week working in the industry for a member of Microsoft and AustCyber's partner network. They will also spend one day a week studying for a Certificate IV in Cyber Security through either TAFE NSW or the Canberra Institute of Technology and gaining relevant Microsoft micro-credentials via Prodigy Learning.

Participants who already hold a Certificate III in Information Technology can apply for credit towards the Certificate IV in Cyber Security.

Leading group training provider MEGT will recruit, employ, and support trainees for the duration of the program.

7.2.3 Immigration

There are barriers that can be immediately resolved through government reforms, especially considering the competition in the global jobs market. In particular, the current migration protocols and wait times need to be quickly adjusted to ensure Australia is a viable candidate for any international expert looking for new opportunities in new places, and do not fall behind in the highly competitive global race for tech talent.

For example, Australian visas for the tech industry take much longer to process compared to our international peers. The permanent Skilled Nominated visa and short-term Temporary Skills Shortage visa currently take between three and six months to process. In contrast, the current approval process for skilled tech workers in New Zealand takes 20 days, 15 days in the United Kingdom, and 10 days in both Canada and Israel.

We understand visa applications have recently been given high priority to healthcare and teaching professions, which are well-deserving and under-resourced. Equally, it is important that processing of critical visa applications including cyber security talent, as well as professionals ranging from ICT specialists to analyst programmers and software engineers, should be similarly elevated in priority. This has become especially important due to the recent major cyber security and data breach incidents. We understand that the current wait times for these applications may have been significantly delayed.

7.2.4 Diversity and inclusion

During Cyber Week 2022, significant discussion focused on the underutilisation of untapped sources for access to talent. Experts noted that there were socio-demographic groups that were not being sufficiently considered.

If appropriately harnessed, they could contribute to the talent shortage challenges and provide invaluable economic and societal benefits. Building diverse teams of people from under-represented and under-served regions and backgrounds, including First Nations people, females and neurodiverse, can boost our innovation and knowledge capabilities to solve problems, bringing with it diversity of lived experiences, skills, values, and perspectives. This also includes people who may not follow traditional educational pathways from TAFEs and universities that might have the right skill sets that are also untapped.

Expert feedback during Cyber Week 2022 discussed these barriers as key reasons for Australia's talent shortage. These reasons have been, and still are, also being widely discussed across the country and our economy, including as part of the Australian Government's Jobs and Skills Summit consultations.

An example of how we are supporting diversity in talent is through Stone & Chalk's recent International Women's Day (IWD) Scholarship which was introduced last year in Melbourne to counter the under-representation of women and minorities in technology. The scholarship will now be rolled out nationally across all Stone & Chalk's Innovation Hubs in 2023, with two scholarships to be awarded in each Stone & Chalk Hub across Adelaide, Sydney, and Melbourne. The six-month program will support founders who identify as women through curated services that drive impact, growth, recognition, and investment. Each recipient will receive exclusive support to scale their businesses, including access to Stone & Chalk's renowned innovation ecosystem of like-minded startup and scaleup founders, while also receiving expert advice tailored to meet individual needs, and introductions to the Group's network of investors, mentors, and more. We need more programs like this across all industries, including cyber security.

Recommendations:

- **Our education system requires ongoing reform to ensure it develops a longer term pipeline of talent, and responsive to the continually evolving emerging tech environment. This should start early at schools and be co-designed in partnership between schools, industry, and governments to build effective school programs around entrepreneurship, innovation, and cyber security and cyber safety. This could entail prioritising appropriate government funding of industry-school partnerships in these domains.**
- **In collaboration with key stakeholders, Australian cyber security leaders have joined forces with us to create the Australian Cyber Security Professionalisation Program (ACSP) to build sustainable career pathways for industry professionals. As this is progressing through its development stage, ongoing government and industry support for this initiative is critical to enable advancement to the next important phase to continue this great work.**
- **Processing of applications for skilled tech workers under the permanent Skilled Nominated visa and short-term Temporary Skills Shortage visa should be benchmarked against our international peers.**
- **Processing of critical visa applications should be extended to cyber security talent, as well as professionals ranging from ICT specialists to analyst programmers and software engineers.**
- **Additional measures to address the backlog of skilled worker visa applications should be explored such as increasing funding support for accelerating the processing of applications and reducing wait times. This may be in the form of recruiting more public service workers and procuring technologies that will expedite the processing of applications.**

- **A specific attraction campaign should be conducted specifically targeting cyber security and other high tech specialist talent overseas in order to increase the quantity and quality of applicants in Australia.**
- **Appropriate government funding should be allocated to bridge diversity and inclusion initiatives that enable access to talent with building innovation ecosystems and cyber security capabilities across Australia. Attached to funding should be clear measures of success and a vision of where we want to be in the short to long term horizon.**

AustCyber
Part of the Stone & Chalk Group

8. Industry and research investment

8.1 Secure-by-Design

- ***Discussion Paper Question #15: How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?***
  a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

Attacks on small to medium sized businesses, including startups, receive less media attention, even though they have just as much to lose or even more.

To ensure the long term success of Stone & Chalk's startups and scaleups, we encourage them to prioritise cyber security. We run workshops specifically designed with Founders in mind, with the clear objective of teaching them how to make and keep their businesses cyber secure. If these businesses want to have a competitive advantage over local and international peers, it must be Secure-by-Design.

The merger of Stone & Chalk and AustCyber in 2021, means we now have a larger more engaged audience, to whom we can clearly demonstrate now the benefits of being part of a Group, where cyber security underpins everything, we offer to our startups, scaleups, corporates and governments. The merger has opened up an opportunity for the cyber security community along with AustCyber's capabilities, to provide a significant cyber security uplift to the emerging technology businesses that are residents at Stone & Chalk.

All these companies, from startups to corporations including their Boards, require education and guidance on how to be cyber secure to future proof their businesses.

More can be done to maximise these activities, and we would welcome ongoing support from government and industry to help support the cyber security uplift for smaller businesses.

8.2 Cyber security sector investment

- ***Discussion Paper Question #16: What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?***

- ***Discussion Paper Question #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?***

We have addressed Questions 16 and 18 together as our responses are interrelated.

In addition to exports to support our Australian cyber security businesses (as discussed above in response to Question 4), startup support, procurement, and R&D investment are other important areas that can be improved upon further.

8.2.1 General comments

Globally, there's a "$2 trillion market opportunity for cybersecurity technology and service providers", according to a McKinsey survey.[12] McKinsey suggests that this opportunity is the result of the disproportionate gap between the rising volume of evolving threats versus low adoption, unmet customer requirements and under-funded company budgets for cyber security products and solutions. It further identifies several key drivers for growing cyber security market potential, including:

- More attacks targeting smaller companies, especially those quickly scaling and exposed to more digital touchpoints.
- The impetus for regulation leading to more demand for cyber security solutions.
- Talent shortages leading to increased demand for outsourced cyber security solutions.

McKinsey suggests providers need to find "productive combinations of product, price, and services that vendors can tailor to target segments and are flexible enough to scale".

In Australia, according to our 2022 AustCyber SCP, the annual revenue growth of the Australian cyber security sector has averaged 8.7% over the past five years, significantly slower than other leading cyber security jurisdictions that have inadvertently grown as a result of geopolitical tensions, ecosystem benefits and strict regulations.

[12] McKinsey, 'New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers' (Article, Oct 2022), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers#/.

Underspending in Australia across several key areas has seen a less globally competitive cyber security sector, diminishing our domestic capability, and presenting both an economic and national security risk.

However, Australia has an opportunity to add $800 million to annual cyber security revenue by 2026 and catch up with our international peers. This will require immediate focus and investment in the sector.

As noted earlier, there are regulatory costs associated with the SOCI Act amendments. While counter-intuitive, the cost of regulation and compliance captured under the SOCI Act could be turned into an enabler for building our cyber security industry.

If not planned already, support could include investment in domestic cyber security solutions to improve cyber security maturity and capabilities of businesses in accordance with relevant cyber security standards. We need to see more businesses and governments investing in products and services from our cyber security startups and scaleups, as well as research, as part of their cyber security uplift.

To gain deeper insights into how AustCyber can help cyber security companies and the industry grow, AustCyber recently undertook market research to gather information, gauging from companies about its needs to create a thriving and sustainable cyber security ecosystem in Australia. Building further from our SCP findings, preliminary high level common themes from our latest survey were:

- Smaller businesses and startups need assistance with tenders to corporates and governments (they do not currently have the resources or the contacts to compete with larger businesses).
- Export remains a key priority with 59% planning to export in 12 months, and 16% already exporting.
- Domestic growth support is required as much as export support as many are looking to expand within Australia.
- Marketing and promotional support is needed, especially those looking to either launch a new product into the market, or to compete with bigger enterprises.
- Connections with government and corporates consistently came up as a pain point, with many seeking our support to use our networks to help make those connections.

AustCyber intends to undertake these market surveys more regularly to ensure that we can hear the views of the cyber security industry and develop strategies to help address their needs, especially in order to grow.

Further assistance from governments and industry to maximise these opportunities would be welcomed. We would also be happy to coordinate and workshop with key stakeholders to explore further how we can immediately support growing the cyber security sector, as part of the Cyber Security Strategy Review.

8.2.2 Startup and scaleup support

The SCP found that cyber security startups in Australia generated 300 times less funding than their international peers, especially in early-stage funding. This is a deep concern for a relatively young industry in Australia that is trying to scale. An additional disadvantage is our comparatively small and immature venture capital market and lack of government investment funding compared to our overseas counterparts.

A question may be asked as to why it is important to invest in Australia's domestic cyber security industry capability. It is important to distinguish between the economic value of investment in the Australian cyber security sector (especially startups and scaleups), versus government assistance for the sake of purely driving sovereign industrial capability without any policy rationale (sometimes labelled as rent-seeking and protectionism). In addition to our SCP findings regarding an $800 annual revenue opportunity, a key point is that startups and scaleups in this emerging tech space are at the leading edge of industry and the future of the digitally enabled economy in Australia. By their nature, investing in startups and scaleups contributes to dynamic efficiency, leading to greater innovations, societal benefits through the creation of more jobs, and economic complexity through the development of new industries. It is therefore critical that these businesses receive appropriate assistance to enable them to quickly grow, which is in the long term interests of the community and economy.

On ways to support innovative Australian startups to succeed (both in cyber security and wider industry), a key reason for the merger between Stone & Chalk and AustCyber is that cyber security should underpin any business that wants to compete and be sustainable in the long term. This is especially critical for businesses in leading-edge emerging technologies (including critical technologies) which is synonymous with innovative startups and scaleups. They will be key to our economy if we want to become globally competitive in the longer term. While it is important to be cyber secure, we need to be more ambitious and be cyber competitive.

To enable greater access to our innovation community, we are currently in discussions with various government agencies and private sector entities for their support to expand our national footprint across Australia, as well as global footprint. If well-designed, there will also be wider community benefits in providing easier access for those in currently under-served and under-represented regions and groups. Federal Government assistance in this area would be more than welcomed. Complementing this, we are also building a national network of AustCyber Australian Cyber Security Innovation Centres with Government support.

8.2.3 Procurement opportunity

It is well-recognised that SMEs represent the largest proportion of businesses, as well as the largest employer, in Australia. Ongoing support for smaller businesses is therefore critical to ensure sustainability of our domestic capability, especially in cyber security.

Our procurement policy also needs to be designed to be flexible to support less established businesses in the emerging tech startup and scaleup space, not just SMEs more generally. These somehow need to be properly factored in when considering regulatory impact, for example, should we wish to develop domestic capability for leading edge technologies and the future of the digitally enabled economy in Australia. If properly designed, local startups and scaleups will have full and fair access to procurement opportunities based on the quality of their products and services in the long term, and not about least costs in the short term.

We therefore welcomed the Government's commitment to supporting SMEs by updating the Commonwealth Procurement Rules (CPR) in mid 2022 to expand opportunities for SMEs and requiring that 20 per cent of procurements by value are sourced from SMEs.[13] We note that this update to the CPR is an increase from the previous 10 per cent threshold. According to estimates by the Department of Finance, the Commonwealth has well exceeded this threshold at 30.8% in 2021-22, which is positive.[14] Nevertheless, it is unclear from these figures the extent to which startups and scaleups, if any, contribute to government procurement - further clarification from this would be welcomed.

[13] Minister for Finance and Minister for Small Business, 'A Better Deal for Australian Businesses Under Commonwealth Contracts' (Joint Media Release, July 2022), https://www.financeminister.gov.au/media-release/2022/07/01/better-deal-australian-businesses-under-commonwealth-contracts.

[14] Commonwealth Department of Finance, 'Statistics on Australian Government Procurement Contracts' (Oct 2022), https://www.finance.gov.au/government/procurement/statistics-australian-government-procurement-contracts-.

We also support the Government's announcement in the 2022-23 Budget for the establishment of the Future Made in Australia Office as part of its Buy Australia Plan. We note that the initiative is intended to build domestic industry capability and improve access to a wider range of businesses including small to medium businesses. For less established startups and scaleups, especially those that are providing leading-edge emerging technologies such as cyber security, it will be important for them to be able to realise these intended benefits in practice.

It should also be acknowledged that at the early stage of these startups and scaleups, they may not always necessarily be considered "value for money" (or least costs) in accordance with the CPR. Therefore, consideration should be given to ensure that building domestic industry capability is not reduced to whether it is least costs in the short term. If necessary, exemptions may need to be provided, for example, to incentivise investment in and procurement of solutions from domestic startups and scaleups. Further exploration into whether the procurement process is startup and scaleup ready would be a worthwhile activity.

Additionally, feedback from the startup and scaleup community is that they prefer being a customer to governments and industry rather than just receiving point-in-time grants that do not offer continuity and deeper partnerships. This can be enabled by building a deep connection to local innovation ecosystems and communities, ensuring lessons learned from the past and opportunities identified for the future have the best chance to take hold and build success.

8.2.4 R&D investment

According to the SCP, R&D government funding support for cyber security decreased by $2.3 million (23%) over the last three years (from $9.8 million in 2019 to $7.5 million in 2022). This is despite the expectations of many that funding should be increasing to meet the evolving cyber security threats to our nation. Interesting to note is that other emerging tech research such as AI received 20 times more investment ($10 million) in 2022, than in cyber security.

There are many emerging technology investment opportunities made available via government funding such as the Australian Research Council (ARC). If funding is being allocated to other critical technologies such as AI over cyber security, this creates a scenario where government funded programs are inadvertently "picking winners". As a result, others are losing out. This unintentionally creates an artificial dichotomy between emerging technologies, where they should instead really be given equal opportunity to dynamically cross-pollinate and produce innovative solutions.

For instance, AI and quantum technologies have featured in cyber security solutions through diversity of ideas. Cyber security should be a foundation for many of our emerging tech startups and scaleups to give them a competitive advantage. If venture capitalists struggle in picking winners, it would be difficult to expect government programs to be any different. Caution therefore needs to be given against prioritising between emerging technology investments, especially around R&D.

We appreciate that this presents a challenge for any government to decide how to allocate funding that supports various emerging tech initiatives including in cyber security. It will be important for the Government to be informed by innovation ecosystem builders like Stone & Chalk Group that have the expertise and experience in enabling and empowering startups and scaleups to grow. We would welcome working with the Government and other key stakeholders to tackle this challenge. For example, development of a national industry development and/or innovation strategy could be an avenue to enable this.

Ultimately, based on our findings, we recommend that the Government should provide additional support for research, innovation, and the development of startups and scaleups in cyber security.

Recommendations:

- **We would welcome ongoing support from government and industry to help support the cyber security uplift for smaller businesses.**
- **Government investment in the cyber security sector has been critical to date. Given the industry's infancy in Australia compared to other more established sectors, it is important that the cyber security sector (especially startups and scaleups) receive ongoing support in growing their businesses.**
- **Early-stage funding in Australian cyber security startups and scaleups should be increased to improve their international competitiveness, supported by access to a larger venture capital market and government investment.**
- **To promote the growth of promising Australian cyber security startups and scaleups, it is recommended that additional project funds are allocated for business growth and cyber security accelerator programs.**
- **As the Future Made in Australia Office establishes itself, we look forward to working with the Government to ensure that procurement of solutions from startups and scaleups, especially in the cyber security industry, are properly supported to succeed and help the Government achieve its procurement policy objectives.**
- **We would welcome further investigation into how the challenges of domestic security responses to cyber security and national security (e.g., amended SOCI Act and Privacy Act,**

and the recently announced Defence Strategic Review that specifically calls out cyber security as a critical domain) can be turned into a positive opportunity to create a competitive advantage for our domestic cyber security capability that can be converted into our global comparative strength.

- **R&D government funding support for cyber security should be increased to be more comparable with other emerging tech investments such as AI in the Australian Research Council (ARC). However, caution needs to be given against prioritising between emerging technology investments. This can be achieved by augmenting R&D funding through ARC grants and by enhancing the scope and transparency of R&D tax incentives, both of which will contribute to the advancement of cyber security research and industry development.**
- **The Government can foster a more robust innovation ecosystem by persisting in collaborating across key stakeholders and by promoting the growth of innovation hubs. It would be beneficial to establish metropolitan and regional cyber security innovation hubs, which can help to encourage innovation, build cyber security communities, and offer a collaborative platform to all key stakeholders in the sector. These stakeholders may include federal and state governments, corporates, international and local cyber security companies, law enforcement agencies, industry bodies, academic institutions, and the general public. In this regard, through the Federal Government's support, AustCyber is establishing its national network of AustCyber Australian Cyber Security Innovation Centres and we would welcome collaborating with stakeholders to provide a meaningful impact as these are rolled out.[15]**
- **Appreciating the challenge of supporting various emerging tech initiatives including in R&D, we would welcome working with Government and key stakeholders to tackle this, for example, through the development of a national industry development and/or innovation strategy.**
- **A workshop (or a series of workshops) should be held with key stakeholders to explore key areas where government and industry could support helping to grow our domestic industry capability in cyber security that provides meaningful and more immediate impact. These could help to unpack further matters including in relation to industry needs such as cyber security startup and scaleup support, procurement support and R&D support, as well as other areas covered in our recommendations (e.g., talent and exports support). As AustCyber is already actively engaged in supporting industry growth, we would be happy to assist the Government in this regard and coordinate with support from key stakeholders.**

[15] See https://www.austcyber.com/national-node-network for further information.

AustCyber
Part of the Stone & Chalk Group

9. Future industry

- ***Discussion Paper Question #17: How should we approach future proofing for cyber security technologies out to 2030?***
- ***Discussion Paper Question #19: How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?***

We have addressed Questions 17 and 19 together as our responses are interrelated.

As noted in our response to Questions 15, 16 and 18, the merger of Stone & Chalk and AustCyber in 2021 highlights that cyber security underpins everything we offer to our startups, scaleups, corporates and governments. The merger has opened up an opportunity for the cyber security community along with AustCyber's capabilities, to provide a significant cyber security uplift to the emerging technology businesses that are residents at Stone & Chalk.

In a recent presentation to the AISA Cyber Security Conference in Canberra, we discussed whether our leaders, including at the Board level, were prepared for tomorrow's cyber security landscape. We especially focused on what the Board and Senior Executives need to think about when considering cyber security and emerging tech trends and investments. As examples, we focused on quantum technology, AI and Web3.

The Board, who are responsible for business decisions on investing in emerging technologies and more generally business transformation, must understand emerging tech trends and know with confidence whether their cyber security is robust enough and leverages those trends.

Established businesses (small to large) and their Board need to continually evolve and invest in emerging technologies complemented with cyber security considerations, whether as part of their products and services, or to enable them to operate and successfully compete locally and globally.

The height of the COVID pandemic over the last few years has required many businesses to accelerate their digital transformation projects, to remain open and competitive virtually in physically constrained conditions.

This increased digitalisation has also presented new and emerging cyber security risks, highlighting the criticality of Boards to remain vigilant and take their responsibility for ensuring good cyber security behaviour very seriously.

It is paramount that we break down any barriers that are preventing Boards (as well as leaders across governments and our wider community) from being aware, informed and educated on cyber security and emerging tech. For the purposes of this response, we will discuss emerging tech examples with respect to quantum technology, AI and Web3.

9.1 Quantum technology

We welcome the news that the Australian Government is consulting and planning to release a Quantum Strategy, with a National Quantum Advisory Committee formed to lead the charge.

9.1.1 State of quantum technology

Several years ago, we might have thought that quantum technology was just a theory or an idea. But a lot has changed since that time. We have several great quantum research activities in Australia,[16] as well as great quantum startups. Currently, one source ranks Australia 8th in quantum research impact, 6th in quantum venture capital investment and 11th in quantum patents.[17] With Australia's great advances in leading quantum research, there is much room to commercialise this research.[18]

According to CSIRO's latest report estimates, Australia's quantum technology opportunity in revenue terms could conservatively reach $2.2 billion by 2030.[19] A proportion of this includes cyber security (under the communications category), estimated to be $400m by 2030, along with an estimated 1,800 cyber security jobs. At a macro level, this is positive news for the cyber security sector, assuming that it integrates with quantum technology opportunities.

[16] Australia's Chief Scientist, 'Dr Cathy Foley Delivers Quantum Australia Conference Keynote 2022' (Keynote speech, March 2022), https://www.chiefscientist.gov.au/news-and-media/dr-cathy-foley-delivers-quantum-australia-conference-keynote-2022

[17] KPMG, 'A Prosperous Future: Emerging Tech Opportunities for Australia and the United States' (Report, Sep 2022), https://kpmg.com/au/en/home/insights/2022/09/prosperous-future-emerging-tech-for-australia-usa-trade.html.

[18] Ibid.

[19] CSIRO Futures, 'Growing Australia's Quantum Technology Industry: Updated economic modelling' (Report, Oct 2022), https://www.csiro.au/en/work-with-us/services/consultancy-strategic-advice-services/CSIRO-futures/Future-Industries/Quantum.

According to QURECA,[20] Australia's investment of $130m in quantum technology is not something to shy away from. That said, we are relatively small players in terms of public and private investment compared to some leading international peers.

Where we cannot globally compete in investment magnitude, it will therefore be important that we leverage on and build our domestic capability through our strategic international partnerships such as AUKUS, Quad Alliance, Five Eyes Alliance, and relationships with other friendly international partners.

The transformational potential of quantum can be significant if it can quickly resolve its research-to-commercialisation dilemma. And there are arguably parallels between quantum and cyber security.

9.1.2 The cyber security implications with quantum technology

Where quantum technology is being considered by businesses for use cases, which is a continually evolving landscape, it will become increasingly important that they consider the technology in terms of cyber security. And we see quantum technology as having profound impacts on the cyber security sector.

Despite this, according to survey responses to our AustCyber's Digital Census 2022 for the Sector Competitiveness Plan (SCP), we asked "In the next 3 years, to what extent will the following trends impact on the cyber security industry in Australia?" Compared to other trends, quantum computing received lower attention in the survey responses.

Quantum computers are expected to be able to decode current cryptography, which would compromise most existing cyber security protections. Many corporate and consumer transactions and commerce depend on the data protection offered by encryption. When quantum computers reach their potential, everything ranging from personal, commercial to classified data will be out in the open, leading to the broadest, deepest hack in history.

[20] QURECA, 'Quantum initiatives worldwide – update 2023' (Jan 2023), https://qureca.com/quantum-initiatives-worldwide-update-2023/.

Several companies are developing "post-quantum cryptography" (PQC) protocols: new encryption mathematics that are immune to the capabilities of quantum machines. Big software vendors will have to build these protocols into their applications. Smaller operations will likely have to do the same or risk exposing all their data to bad actors. These new standards must spread across every device and service that transmits encrypted data.

According to the RAND Corporation, in many ways, the threat analogy has been drawn with the Y2K Millennium Bug, where the risk related to the global information and communication infrastructure and federal leadership and partnerships were key to success in managing the risks.[21] There are of course differences in not knowing the specific date when the quantum technology risk might occur and the threat could arise from existing vulnerabilities exploited by a sophisticated, capable adversary. Is it even here already?

The subject is beginning to become topical for the businesses when The Economist starts covering it:[22] "A survey of experts, conducted in 2021, found a majority believed that by 2036, rsa-2048, an existing industry-standard encryption protocol that makes use of keys 2,048 bits long, could be broken within 24 hours."

More urgent threats come from "harvest now, decrypt later" attacks, where encrypted data is collected in volume for decryption when quantum technology is available. Though today's social media posts are unlikely to interest a hacker from the future, plenty of data - medical records or national security communications - might retain their value.

An important reference is the ACSC website.[23] On the subject of PQC, there is relatively limited ACSC information because of its "newness". Essentially, the ASD/ACSC are monitoring developments in this area, but recommend companies research, test, and conduct practical trials and work with vendors and researchers.

---

[21] RAND Corporation, 'Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption' (Research Report, 2020), https://www.rand.org/pubs/research_reports/RR3102.html.
[22] 'How to preserve secrets in a quantum age' (The Economist article, Jul 2022), https://www.economist.com/science-and-technology/2022/07/13/how-to-preserve-secrets-in-a-quantum-age.
[23] ACSC, 'Planning for Post-Quantum Cryptography' (July 2022), https://www.cyber.gov.au/acsc/view-all-content/publications/post-quantum-cryptography.

The first challenge for many Boards is that if they have not considered quantum technology at all as a business use case, they will also need to consider it as a business risk case.

The US Cyber Infrastructure & Security Agency has released its own advice in August last year on "Preparing Critical Infrastructure for the Transition to Post-Quantum Cryptography" along with a roadmap by NIST and the US Dept of Homeland Security - while not Australian, it might be a useful reference.[24]

We note that US President Joe Biden has already signed into law late last year, the Quantum Computing Cybersecurity Preparedness Act - the law sets the US Office of Budget Management the task of complying with updated security advice from the NIST regarding "post-quantum cryptography standards".[25] This law also means federal agencies will be required to keep an up-to-date inventory of any IT systems that are vulnerable to quantum decryption methods as a part of this guidance. It remains to be seen whether Australia will follow suit in its quantum cyber security preparedness.[26]

9.2 AI

AI continues to play an increasing role in cyber security and alongside quantum technology will see an interesting period of convergence between various emerging technologies.

For example, AI has been deployed to scan through code more quickly than a human being, which has made it easier to detect attacks. Of course, both sides can deploy AI, but this only increases the urgency for corporates and governments to invest to ensure they have access to the best algorithms trained on the right data.

[24] CISA, 'CISA Releases New Insight on Preparing Critical Infrastructure for the Transition to Post-Quantum Cryptography' (Press release, Aug 2022), https://www.cisa.gov/news-events/news/cisa-releases-new-insight-preparing-critical-infrastructure-transition-post-quantum-cryptography.

[25] 'President Biden signs Quantum Computing Cybersecurity Preparedness Act' (Cyber Security Connect article, Dec 2022), https://www.cybersecurityconnect.com.au/critical-infrastructure/8545-president-biden-signs-quantum-computing-cybersecurity-preparedness-act.

[26] '2023 is the year Australia must begin to prepare for quantum threats' (Cyber Security Connect article, Feb 2023), https://www.cybersecurityconnect.com.au/policy/8726-2023-is-the-year-australia-must-begin-to-prepare-for-quantum-threats.

The last several months in the world of AI has been arguably disruptive. It was only at the end of November last year that OpenAI launched ChatGPT (a generative pre-trained transformer), shortly followed by $29bn USD valuation and $10bn USD investment by Microsoft in the last month. Since then, it has now progressed to the next iteration (GPT-4 released in March this year) which has received increasing public attention.

While past discussions in the Board about AI have been along a similar vein as other emerging technologies like quantum technology and understanding its business use case, ChatGPT is presenting practical examples that can be realised now and easily accessible in the workplace and others.

For an application that has only been accessible to the community in such a short period of time, it is an interesting experiment in societal behaviour, which has divided opinion. We have seen a lot of commentary from experts, governments, schools, and others across our community about both the pros and cons, leading to bans in some workplaces, schools and even conferences, while others have embraced its use in some shape or form. We are now seeing an enterprise version of ChatGPT, and it will be interesting to see how that unfolds in workplaces and even amongst hackers.

There have been examples and discussions of different ways in which hackers can leverage ChatGPT in how to write better malware code and potentially more convincing socially engineered phishing messages or strategies.

While the platform and other similar ones have their limitations, it will continually evolve as its design to be trained and improved, which can be used for both good, bad or neither. Previous ethical considerations around AI will need to be revisited again to see whether they are still appropriate in this latest example.

For the Board, they will need to be reminded that this is another newer and openly accessible avenue in which hackers can use another tool at their disposal to generate malware, phishing, and other malicious attacks.

9.3 Web3

We are seeing a world that is shifting from a centralised and closed environment to one that is open and decentralised. Everything the internet did to music or newspapers is now happening to everyone else. This includes finance, energy, education journalism and space. They say that it could unbundle the incumbent banking industry and reinvent insurance, as well as digital government services.

Web 3 is the next anticipated phase of the internet, featuring a decentralised internet allowing for greater user control of their data. With increased focus on decentralisation and privacy and security features in Web 3, this should be positive in cyber security terms. However, businesses will need to adapt accordingly so that they are Web3 ready.[27]

The impact of Web3 needs to be properly understood by the Board and their businesses whose products, services or businesses are based on a Web 2.0 centralised architecture. Specifically, they will need to determine whether they will be decentralised Web3 capable.[28]

In our view, we can see that despite current market challenges, the growth of Australia's Web3 community has not been stifled with the volume of talent and innovation in the future of Web3, digital assets and blockchain technologies remaining strong. We are currently exploring this through Stone & Chalk's new Web3 Innovation Centre where we support Web3 founders and their businesses navigate shifting market and economic conditions, bringing public and private sectors together to unlock the industry's capabilities.

These are just some examples of emerging technologies where cyber security is a critical part of the discussion and can't be considered in isolation. If leaders do not properly understand and plan for the emerging tech threats and opportunities, especially as they may be impacted by evolving cyber security threats, they may not only risk falling behind but also be exposed to new risks in the near future.

Recommendations:

- **We would welcome working with the Government and other key stakeholders to review cyber security related issues associated with emerging tech.**
- **Further review should be given to Australian preparedness for the cyber security implications of emerging tech such as quantum technology, AI and Web3.**

[27] 'Web 3.0 and Its Cybersecurity Implications' (RSAConference blog, Nov 2022), https://www.rsaconference.com/library/blog/web-30-and-its-cybersecurity-implications.
[28] 'The $10 Trillion Case For Decentralized Cybersecurity' (Forbes article, Feb 2023) https://www.forbes.com/sites/lawrencewintermeyer/2023/02/02/the-10-trillion-case-for-decentralized-cybersecurity/?sh=2c2e5b9459da.