Governance Institute of Australia

T +61 2 9223 5744 F +61 2 9232 7174
E info@governanceinstitute.com.au
Level 10, 5 Hunter Street, Sydney NSW 2000
GPO Box 1594, Sydney NSW 2001
W governanceinstitute.com.au

1 November 2019

Cyber Security Policy Division
Department of Home Affairs

By email: artificial.intelligence@industry.gov.au

Dear Sir/Madam

Australia's 2020 Cyber Security Strategy: A call for views

Governance Institute of Australia (Governance Institute) is the only independent professional association with a sole focus on whole-of-organisation governance. Our education, support and networking opportunities for directors, company secretaries, governance professionals and risk managers are unrivalled.

Our members have primary responsibility for developing and implementing governance and risk frameworks in public listed, unlisted and private companies. They are frequently those with the primary responsibility for dealing and communicating with regulators such as the Australian Securities and Investments Commission (ASIC) and the Australian Prudential Regulation Authority (APRA). In listed companies, they have primary responsibility for dealing with the Australian Securities Exchange (ASX) and interpreting and implementing the Listing Rules. Our members have a thorough working knowledge of the Corporations Act 2001. Our members also play an important role in external reporting by public listed, unlisted and private companies. We have drawn on their experience in providing our feedback.

Governance Institute welcomes the opportunity to comment on the Paper Australia's 2020 Cyber Security Strategy: A call for views (Paper).

We commend the Government on the Paper. Cyber security affects all Australians. Many of our members are working as governance and risk professionals in a range of organisations, from the largest listed companies responsible for critical infrastructure to small businesses and not-for-profits. In a recent Governance Institute research Report three quarters of online survey respondents identified the impact of technology disruption as one of the three key trends likely to impact on their role in the next five years.[1] For this reason our members consider it is critical for organisations to have proper governance around cyber security risk management.

Governance Institute is currently involved in a joint research project with CSIRO Data 61 on digital trust.[2] The preliminary findings of the quantitative survey indicate that cybercrime is one of the top two issues that keep survey respondents up at night. Cybersecurity is a foundational aspect of building digital trust. Digital Trust will be vital for Australian businesses and consumers to manage the risks and opportunities of the digital age.

Our members consider it is vital that governments, academics, civil society, businesses and the community work collaboratively to strengthen national cyber resilience. They also consider it is

[1] The future of the governance professional, Governance Institute of Australia, August 2019.
[2] Research results to be released February 2020.

important not only to acknowledge the risks in this area, but also the opportunities for Australia to develop and export expertise in cyber security capability.

This submission makes some general comments on the issues raised by the Paper.

1. Preliminary - What is your view of the cyber threat environment? What threats should Government be focusing on?

Our members consider a useful way of considering the range of cyber threats involves looking through different lens – individuals, small business, corporations and public sector entities. Each of these groups have unique cyber issues, although many of the threats are common across these different groups.

- Threats to individuals include:
    - cyber-bullying
    - failure to read or understand long and complex terms of use
    - identity theft, and
    - the power of digital platforms
- Threats to small business and corporations include:
    - denial of service attacks
    - identity theft
    - data breaches and information theft
    - data encryption, and
    - tricking customers and others into making illegitimate payments
- Threats to public sector entities are the same as those identified above, but present an opportunity for government to be more demanding in terms of compliance with policies and standards.

Our members consider that given the pervasive nature of the cyber threat environment there needs to be a coordinated effort across all groups, although given their roles our members' comments are primarily focused on threats affecting small business, corporations and the public sector.

2. Organisational ownership of cyber security risk

The most recent edition of the ASX CGC's Corporate Governance Principles and Recommendations (Corporate Governance Principles and Recommendations) explicitly acknowledges the importance of an organisation's risk management framework dealing adequately with cyber-security risk.[3] Recognising and managing risk is a key aspect of the governance of organisations and a board's oversight role. While the Corporate Governance Principles and Recommendations are directed at listed entities they are the leading Australian statement on corporate governance and influence the governance practices of Australian organisations of all types. Responsibility for managing the risks posed by cyber is an important part of the governance of risk in organisations.

Board responsibility for cyber security in APRA regulated entities is also explicitly addressed in APRA *CPS 234 Information Security* (CPS 234). CPS 234 is intended to ensure that APRA-regulated entities take measures to be resilient against information security incidents (including cyberattacks) and provides that the boards of these entities are ultimately responsible for information security. Under CPS 234 these entities must clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals.

---

[3] Commentary to Recommendation 7.2, *Corporate Governance Principles and Recommendations*, 4th edition, 2019, ASX Corporate Governance Council at page 27.

In many other organisations responsibility for cyber security risk remains the domain of the IT department. Cyber security breaches can occur in organisations of all kinds and our members consider that cyber security needs to be understood as an important part of any organisation's risk management framework.[4] Given the dependence of almost all staff in all areas of a business on use of the internet, the responsibility for cyber security needs to become mainstream in organisations in the same way that responsibility for data privacy is now widely accepted as a universal responsibility with appropriate board oversight. While cyber security remains the responsibility of the IT department in organisations and has a low risk profile it will not attract the funding and resources needed.

Organisations such ours play an important role in promoting best practice and encouraging a holistic approach to governance and risk. Strategic partnerships with organisations such as ours, through targeted campaigns, could help to embed cyber security risk as an organisational wide issue with senior leaders, executives and upskilling of Boards in understanding critical infrastructure risks and their cyber risk appetite[5].

Governance Institute recommends that cyber security needs to be seen as whole-of-business risk management issue and become a standing agenda item for organisations' governance committees. Cyber security awareness needs to become part of organisations' risk management culture. **Governance Institute also recommends** strategic partnerships with organisations through targeted campaigns to help embed cyber security risk as an organisational wide issue.

3. Building a network of skilled professionals

Our members consider it is critical to maintain and expand on efforts to increase understanding and awareness of cyber security in all organisations. In 2017, Australian companies predicted '…*17% of cyber security positions advertised would go unfilled.*.'. [6] This is not unique to Australia and there is in fact a worldwide deficit of cyber security skills … 'The reality is that there are simply not enough skilled humans available to properly plan, manage, integrate, and optimize security devices, strategies and protocols.'[7]

A recent study on the role of boards in driving organisational innovation found, amongst other things, that Australian directors are not prioritising innovation or disruption risks to the extent seen in overseas boardrooms, suggesting Australian boards underestimate looming strategic risks. The Study also found Australian boards lack critical technical and innovation skills and that more must be done to broaden the talent pool.[8] Our members consider that the level of awareness of the importance of cyber security is for many organisations and boards at a formative stage. This needs to change.

As governance and risk professionals our members often play a key role in highlighting to boards, areas where boards may require additional skills or emphasis. One area our members have highlighted is the difficulty of locating appropriate materials and training. While there have been a number of initiatives such as the Academic Centres of Cyber Security Excellence

---

[4] *Your whole business is basically gone*, Sydney Morning Herald, 23 October 2019.
[5] https://www.aspi.org.au/report/protecting-critical-national-infrastructure-era-it-and-ot-convergence
[6] See https://ministers.pmc.gov.au/tehan/2017/new-program-build-australias-frontline-cyber-security-workforce, February 2017.
[7] *Here's how we can tackle the growing cybersecurity skills gap*, World Economic Forum, Agenda, 23 January 2019.
[8] *Driving Innovation The Boardroom Gap*, September 2019, Australian Institute of Company Directors.

established by Government, , established as part of the 2016 Cyber Security Strategy and the commitment of $1.9M in funding, much more remains to be done and the level of take up outside specialist discipline remains low.

Our members consider that there is a need to support innovative programs aimed at addressing the skills shortage, for example collaborations between businesses and universities.[9] Our members also see a need for education and training to embed cyber security skills in governance professionals such as risk managers and internal audit. This is key given the important role they play in risk management. Our members report that while there are a number of cyber security courses and certifications in the market, it can be difficult to determine the most appropriate training. In many cases training is only accessible through a specialisation within a tertiary course.

Our members also consider one area where Government could play a role is independent guidance on the best cyber security qualifications for various levels of need. Initiatives similar to the Government's focus on the importance of STEM might be useful.

If there is an urgent need to increase education and awareness in this area, this also represents an opportunity for Australia to lead the world in developing cybersecurity professionals and expertise and to export these skills globally. Australia can play a key role in developing new training and education courses, and promoting cybersecurity as a future career, noting that this is a longer term solution and the need for these skills is increasing exponentially

Governance Institute recommends that one area where Government could play a role is independent guidance on the best cyber security qualifications for various levels of need. Initiatives similar to the Government's focus on the importance of STEM might be useful. **Governance Institute also recommends** that Government consider the key role Australia can play in developing new training and education courses, and promoting cybersecurity as a future career, noting that this is a longer term solution and the need for these skills is increasing exponentially.

4. Regulation

While there is an existing regulatory framework in place including the Privacy Act, APRA Standards and ASIC and the Corporations Act, the evidence suggests that the status quo will be ineffective in the long term. Our members consider that it is virtually impossible for a regulatory response to be sufficiently agile to address the pace of change in cyber threats.[10] Any approach to regulation will need to be multi-faceted involving a combination of approaches: 'black-letter' law, industry standards (local and international), inter-governmental and industry codes. It will be critical for the Australian Government to work cooperatively with other governments in this area.

Governance Institute recommends a multi-faceted approach to regulation involving a combination of approaches and that the Australian Government work cooperatively with other governments in this areas.

5. Consumer awareness

Given that cyber incidents are increasing in frequency and impact, ongoing consumer awareness is critical. **Governance Institute recommends** that Government continue to build on the work it has already done to make citizens more cyber aware and to take active steps to protect themselves from cyber risks.

---

[9] For example secedu, the collaboration between Commonwealth Bank of Australia and the University of New South Wales.

[10] Privacy Act and the Office of the Australian Information Commissioner, APRA CPS 234 and section 912A of the Corporations Act and ASIC *Report 429 Cyber resilience: health check*.

6. Investment

Our members consider that there has been considerable investment in cyber security policy. The Essential 8 developed by the Australian Signals Directorate is an excellent document. Similarly, the ISO 27000 series provides a good baseline for cyber security.

Despite the existence of these tools and frameworks, vulnerabilities arise because of the lack of funding and investment for the tools to support implementation of the key controls necessary to defend against, detect and remediate cyberattacks. For example, while assistance is available for cyber security for small business through the Government small business program to assist them to identify vulnerabilities, what is still required is the funding to address these vulnerabilities. This also applies at the government level – departments have programs to implement policy around the Essential 8 and the ISO 27000 series but do not necessarily have the budget allocation to acquire the tools required. The lack of funding is in part related to cyber security still being perceived to be the realm of the IT department rather than a whole-of-organisation risk.

Governance Institute recommends that Government consider the opportunities for Australia businesses that operate in the cybersecurity space and how their efforts can be supported and augmented through government assistance.

If you have any questions concerning this submission or would like to discuss any aspect please contact our General Manager, Policy and Advocacy, Catherine Maxwell.

Yours sincerely

Megan Motto
CEO