Governance Institute of Australia

T +61 2 23 5744 **F** +61 2 9232 7174

E info@governanceinstitute.com.au

Level 11, 10 Carrington Street,

Sydney NSW 2000

GPO Box 1594, Sydney NSW 2001

W governanceinstitute.com.au

14 April 2023

Cyber, Digital and Technology Policy Division
Department of Home Affairs
6 Chan St
BELCONNEN ACT 2617

Dear Sirs,

2023 – 2030 Australian Cyber Security Strategy

Governance Institute of Australia

Who we are

Governance Institute of Australia (Governance Institute) is a national professional association, advocating for our network of 43,000 governance and risk management professionals from the listed, unlisted, public, not-for-profit and charity sectors.

As the only Australian provider of chartered governance accreditation, we offer a range of short courses, certificates and postgraduate study. Our mission is to drive better governance in all organisations, which will in turn create a stronger, better society.

Our members have primary responsibility for developing and implementing governance frameworks in public listed, unlisted and private companies, as well as not-for-profit organisations and the public sector. They have a thorough working knowledge of the operations of the markets and the needs of investors. We regularly contribute to the formation of public policy through our interactions with Treasury, the Attorney General's Department, the Department of Home Affairs, ASIC, APRA, ACCC, ASX, ACNC and the ATO.

Our activities in this area

Governance Institute members have both a strong interest and involvement in digital technology and cyber security policy and take the governance and risk management of privacy, data protection and cyber security in all sectors very seriously. We have advocated for some time for digital transformation and modernisation in many areas of corporate regulation, including supporting virtual and hybrid AGMs, digital document execution, digital shareholder communications, and the introduction of Director ID numbers. Many of our members work as governance and risk professionals in a range of organisations that are part of or connect with the digital economy, from the largest ASX-listed companies responsible for critical infrastructure to small businesses and not-for-profits , who are nonetheless affected by cyber issues. They are experienced

in considering the industry and economy-wide implications of cyber security, data and technology governance and digital transformation.

Governance Institute is a founding member of the ASX Corporate Governance Council, which produces the leading Australian statement on corporate governance, the Corporate Governance Principles and Recommendations. Recommendation 7.2 of the 4th edition explicitly acknowledges the importance of an organisation's risk management framework dealing adequately with privacy and data breaches, cyber security risks, and digital disruption.[1] We strongly supported this inclusion. While the Corporate Governance Principles and Recommendations are directed at listed entities, they influence the governance practices of Australian organisations of all types and in all sectors.

We produce a range of thought leadership and industry guidance in relevant areas. In recent years Governance Institute's Risk and Technology policy committee has published Good Governance Guides on the topics of cloud services, digital transformation, digital trust, technology strategy, technology governance, cyber security, data as an asset, and ethical use of artificial intelligence. Our 2020 Report on the future of the risk management professional identified cyber security, artificial intelligence and digital disruption as key trends likely to impact on risk management professionals by 2025.[2] In 2021, our Report on the future of the board, found that cyber security and data privacy security are two of the biggest challenges associated with technological disruption facing boards of directors into the future.[3]

We regularly contribute to consultations on digital themes including our submission on Australia's 2020 Cyber Security Strategy and our 2021 Submission to the consultation on strengthening Australia's cyber security regulations and incentives. We also made a recent Submission to the review of the Privacy Act which has significant implications for this consultation. In our capacity as a division of The Chartered Governance Institute (CGI), an international body with over 30,000 members worldwide we also contribute to the international debate on digital technology and data governance issues.

In our members' experience many Australian businesses have rapidly increased their cyber resilience, posture and awareness in recent years. This has been particularly apparent since the COVID-19 pandemic, and the boards of Australian companies of all sizes are increasingly aware of cyber security, data protection, privacy, and related issues. Ransomware attacks, data sovereignty, the risks associated with widespread use of cloud services, and many other related topics are frequently discussed at our policy committee meetings. These are clear and present themes on the minds of governance and risk management professionals across Australia and on the agendas of the boards they support.

This Submission does not respond to all of the questions set out in the Discussion Paper but to those of interest and concern to our members.

Executive summary

- Governance Institute's members welcome the opportunity to make this submission on the critical issue of cyber security. We support the aims of the Government in working towards creating a secure economy and thriving cyber ecosystem that protect consumers, keeps pace with rapid technological change, and promotes good governance and risk management in organisations.
- We encourage all levels of government to coordinate to ensure better harmonisation and greater simplicity between cyber security, data breach, data sovereignty, critical infrastructure and privacy regulation.

[1] ASX 2019, Corporate Governance Principles and Recommendations 4th Edition, p. 27.
[2] Governance Institute, 2020, *Future of the Risk Management Professional*, p. 19.
[3] Governance Institute, 2021, *Future of the board*, p. 10.

- We recommend the development of a well-designed, well-targeted and fit for purpose cyber governance standard supported by guidance suitably tailored for organisations of differing sizes.
- We recommend against further reform or expansion of the Security of Critical Infrastructure Act at this stage.
- We consider the range of existing directors' duties and obligations under the Corporations Act, the common law and company constitutions (where applicable) are sufficiently broad to adequately cover care and diligence obligations relating to cyber security.
- We consider there is currently no demonstrated need for a stand alone Cyber Security Act and that the Government consult further on any proposal to introduce such an Act.
- We acknowledge the attraction of a prohibition on the payment of ransoms by both victims and insurers in response to extortion demands but consider there are a range of practical issues that warrant further consideration.
- We recommend a concerted whole-of-Government approach to cyber security and data governance to secure government systems.
- We recommend evaluation measures such as regular reports on trends and good practices as good methods of supporting public transparency and input.

Legislative and regulatory reforms

We have the following comments on the proposals for regulatory and legislative reform set out in the Consultation Paper:

- **Harmonisation of existing requirements** - our members agree that 'businesses do not find that their cyber security obligations are clear or easy to follow, both from an operational perspective and as company directors'.[4] In our 2021 Submission we identified at least 15 pieces of legislation, voluntary industry standards and potential future regulation potentially applicable to Australian businesses in this area, which are administered by a wide array of Government departments, regulators, agencies and industry associations.[5] This number has not decreased and leaves industry and consumers facing a 'spaghetti' of regulatory obligations and standards at a time when cyber attacks and 'cyber anxiety' are at an all time high. We encourage all levels of government to cooperate to ensure better harmonisation between cyber security, data breach, data sovereignty, critical infrastructure and privacy legislation.

- **Mechanism for reforms** – our members have previously expressed in principle support for a voluntary cyber governance standard for large businesses, provided it is well-designed, well-targeted and fit for purpose, noting that many sectors and entities are already heavily regulated in this area.[6] They consider that a standard could also be helpful for smaller businesses. Any standard should be supported by guidance suitably tailored for organisations of differing sizes. The Office of the Australian Information Commissioner's (OAIC) Guidance on Privacy Impact Assessments is a good example of this type of guidance.[7] It would be important for any standard to find a 'home' within an appropriate framework and under the authority of an appropriate regulator or agency with the relevant areas of expertise. This will require careful coordination by Government, Federal, State and Territory having regard to the various overlapping areas of policy, areas of law, the various programs of work currently underway by different areas of government, and the wide array of regulated entities and affected stakeholders.

---

[4] See Consultation Paper page 17.

[5] See Submission Strengthening Australia's cyber security regulations and incentives, Governance Institute of Australia, August 2021, pages 4 – 5.

[6] See Governance Institute Submission August 2021 at page 2.

[7] See OAIC website.

- **Further reform of the Security of Critical Infrastructure Act** (SOCI Act) – the extensions to the SOCI Act have only come into effect relatively recently with the Risk Management Program Rules commencing in February 2023. Our members consider this program of legislative reform should be subject to a period of 'bedding down' and evaluation of how the extension of the SOCI Regime operates in practice before further extending the regime to cover areas such as customer data and systems. The current review of the Privacy Act is also likely to impact on customer data in a range of ways. It will be important to consider the Privacy Act Review and any extension of the SOCI Regime to customer data in tandem.

- **Obligations of company directors** - we have previously urged a cautious approach to expanding director liability in response to specific emerging issues such as cyber security risks.[8] Our members consider the range of existing directors' duties and obligations under the Corporations Act, the common law and company constitutions (where applicable) are sufficiently broad to adequately cover care and diligence obligations relating to cyber security. They consider that particularising directors' duties runs the legal risk of limiting the scope and operation of the existing general duties. For example, it now appears settled that in order to comply with existing duties, diligent company directors ought to be considering climate change risks and that directors' existing duties are sufficiently broad to cover these risks.[9] Our members consider cyber security risks are similar and directors' existing duties already incorporate these risks. ASIC, the corporate regulator has also been proactively promoting the importance of cyber resilience to Australian companies for some time.[10] It has already successfully prosecuted an Australian financial services licence holder for failure to manage cybersecurity risks as part of its licence obligations.[11] The standard expected of directors of Australian entities is already high by international comparison and there is a noticeable trend towards imposing greater personal liability on directors, and recent cases suggest that Australia's corporate regulators are increasingly willing to pursue civil and criminal action against directors. Our members also note that the cost of Directors' and Officers' (D&O) insurance has increased substantially in recent years in all sectors. This cost increase has been directly observed by our members who are company secretaries, as board-related costs frequently sit in the company secretary's cost centre. Further expansion of director liability may risk additional cost escalation in the D&O insurance market. Our members consider that the existing obligations of company directors are adequate to address cyber security risks and consequences. The placing of Cyber Insurance for directors and officers has seen the same cost pressures based on claims.

- **Stand alone Cyber Security Act** –there is a once in a generation review of the Privacy Act. The ACCC Digital Platform Services Inquiry is in progress as well as a range of other Government priorities. Our members do not consider there is a demonstrated need to introduce a stand alone Cyber Security Act. They also consider the need for, and coverage of, a specific Act would need to be the subject of extensive consultation to ensure any legislation serves to simplify a current cyber security legislative regime rather than add to the already complex web of legislaton and Standards.

- **Ransom payments and extortion demands** – our members acknowledge the attraction of a prohibition on the payment of ransoms by both victims and insurers in response to extortion demands. However, they consider there are a range of potential practical issues which warrant further consideration. One of these is that in almost all cases cyber criminals reside overseas well beyond the reach of Australian law enforcement. This means that even though a ransom payment may be

[8] See our August 2021 Submission at page 6.

[9] The Centre for Policy Development.

[10] See the resources at https://asic.gov.au/regulatory-resources/corporate-governance/cyber-resilience/.

[11] See ASIC MR 22-104 Court finds RI Advice failed to adequately manage cybersecurity risks.

prohibited under Australian law this is unlikely to have any real impact on overseas resident cyber criminals who, depending on their movitation, are likely to increase the scale and ferocity of their activities and resort to other means of profiting from their gains such as selling data on the dark web. Some commentators have warned that banning payments would 'encourage threat actors to go after targets where there will be the most impact, and in most cases that means not just the impact on the organisation itself, but impact on the broader community.'[12] Where a ban on ransoms is to be introduced, there may need to consideration of a 'carve out' for example, in situations where personal safety or the health and welfare of individuals are involved.

- **Commonwealth Government departments and agencies demonstration of cyber security best practice** – the scale of recent cyber attacks has demonstrated that far too many organisations including Commonwealth Government departments and agencies hold unnecessary amounts data for much longer than they need. Our members consider there needs to be a concerted whole-of-Government approach to cyber security and data governance to secure government systems. Projects to improve verification of individuals' identity by Government agencies and departments need to be fast tracked as well as greater use of current iniatives such as the newly introduced director ID, a verified method of identifying an individual or myGovID which could be used for a greater range of purposes.

- **Evaluation measures to support public transparency and input** – our members consider that some of the most helpful information Government can provide are reports such as ASIC's six-monthly Corporate Finance Update or the OAIC's six monthly reports on data breaches. These reports provide information on trends and good practices which are of assistance to organisations. Given how rapidly events move, monthly reports on these issues would be of assistance.

Please contact me or Catherine Maxwell, GM Policy and Research if you have any questions in connection with this submission.

Yours faithfully,

Megan Motto

CEO

[12] See Top law firm warns banning cyber ransom payments will backfire, AFR, 28 November 2022.