Adelaide Law School

SUBMISSION ON AUSTRALIA'S 2023 – 2030 CYBERSECURITY STRATEGY

Dr Samuel White

Elizabeth Watford

Professor Matthew Stubbs

Associate Professor Beth Nosworthy

About this Submission

Thank you for the opportunity to respond to the Discussion Paper on the 2023-2030 Australian Cyber Security Strategy. We are academics and a student researcher from the University of Adelaide Law School, and members of the University of Adelaide's Research Unit on the Regulation of Corporations, Insolvency and Taxation (ROCIT) and the Research Unit on Military Law and Ethics (RUMLAE). This submission will focus on regulatory reform by responding to aspects of the following questions from the Discussion Paper.

Question 1: What legislative or regulatory reforms should the Government pursue to enhance cyber resilience across the digital economy?

The economic benefits of open access data are yet to be fully realised in Australia. However, in order to do so safely and securely, legislative and regulatory reform is necessary. We suggest a harmonised approach in order to mitigate possible vulnerabilities within cybersecurity across individuals, business and government. In order to do so, some suggested reforms include conducting a cybersecurity maturity review, and harmonising regulatory protections around the use and storage of data.

Question 1(c): Should the obligations of company directors specifically address cybersecurity risks and consequences?

The challenges of cybersecurity necessitate an update to regulatory frameworks around corporate director obligations and duties. To mitigate against the difficulties of using the 'stepping stone' approach to director accountability, we suggest mandatory penalties be introduced for company directors who fail to address cybersecurity risks, with the insertion of direct, personal liability for directors who fail to fulfil their duty of care and diligence leading to cyber breaches, breaches similar to liability of directors for insolvent trading under s 588G of the *Corporations Act 2001* (Cth).

Question 1

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

Australia's 'patchwork of policies', laws, and visions are not in line with the current challenges presented by the digital age.[1] Policymakers have the difficult task of balancing how Australia's data can be opened to progress the data economy, whilst maintaining strong cybersecurity measures. The Australian Government has presented potentially conflicting views on the juxtaposition between cybersecurity and an open-data economy. The Department of Industry, Science and Resources' agenda is to 'enable responsible and transparent access to data (with appropriate data safeguards) to support the data economy';[2] whereas the Honourable Clare O'Neill MP, Cybersecurity and Home Affairs Minister, wants Australia to be the world's most cyber secure country by 2030.[3]

In 2022, 65% of global gross domestic product (GDP) is expected to be digitised, illustrating the breadth of economic opportunity and necessity of data crossing borders.[4] Enhancing access to data has also been identified as a top five priority for the digital economy amongst Organisation for Economic Cooperation and Development (OECD) countries.[5] Ultimately, opening Australia's data would help make the country an attractive destination for data and digital-related investment,[6] and help reduce loss of talent overseas.[7] The key is to ensure that the growth of the data economy (through opening data) does not come at the cost of cybersecurity. The Australian Cybersecurity Strategy stated: 'a digital economy relies on the ability to trust that our personal data, infrastructure, and underpinning systems are secure'; this statement highlights that before Australia can contribute to an open data economy, the critical infrastructure and foundations for cybersecurity must be laid first, in both government and industry.[8]

---

[1] 2023-2030 Australian Cybersecurity Strategy Discussion Paper, 4.
[2] Department of Industry, Science and Resources, *Australia's Tech Future: Delivering a strong, safe and inclusive digital economy ('Australia's Tech Future Publication')* (Data and Publication, 2018), 34.
[3] 2023-2030 Australian Cybersecurity Strategy Discussion Paper, 4.
[4] Daniel S Hamilton and Joseph Quinlan, *Transatlantic Economy 2022* (Publication, 2022), 44.
[5] Craig Gibson et al, 'Leaked Today, Exploited for Life' (White Paper, Trend Micro Research, 18 October 2022), 3.
[6] Marcel Boer, 'Open-Source Data Platforms', *Medium* (Website, 24 May 2020), <https://medium.com/swlh/open-source-data-platforms-b3b4768f9e3e>.
[7] Marcel Boer, 'Open-Source Data Platforms', *Medium* (Website, 24 May 2020), <https://medium.com/swlh/open-source-data-platforms-b3b4768f9e3e>.
[8] 2023-2030 Australian Cybersecurity Strategy Discussion Paper, 10.

In terms of preventative measures, the Oceania Cybersecurity Centre has urged the Australian Government to conduct a cybersecurity maturity review (CMR), which examines the nation's policy and strategy, culture and society, knowledge and capabilities, legal and regulatory frameworks, and standards and technologies.[9] Conducting a CMR provides a sound basis to identify what reforms are necessary and their anticipated impact.[10] A CMR would provide the Australian Government with a roadmap on cybersecurity policy, and at present, a CMR has not been conducted.[11]

The breadth of legislation that revolves around cybersecurity and data is overwhelming. The vast number of regimes that industry is required to follow makes it hard for obligations to be identified and followed. Cybersecurity obligations exist in the *Privacy Act 1988* (Cth), *Corporations Act 2001* (Cth), *Criminal Code Act 1995* (Cth), and *Online Safety Act 2001* (Cth), to name a few. Regulators including the Office of the Australian Information Commissioner (OAIC), the Australian Competition and Consumer Commission (ACCC), Australian Securities and Investments Commission (ASIC) and the Australian Prudential Regulation Authority (APRA) are all also overseeing risks and potential prosecutions within the cyber arena. A harmonised approach is recommended for industry to fully understand which provisions apply to them, what definitions to follow, and subsequently the practical application of their relevant cyber obligations. A harmonised approach would also assist the public to understand which rights they can exercise if they are caught up in a cyber breach.

More specifically, professionals within organisations, such as data scientists and marketing professionals, need to be adequately trained to utilise data in a way where the organisation can extract important information, but then dispose of it when it is no longer needed. Without a clear use or governance plan, the collection and publishing of data on open sources can result in increased costs and liability greater than the potential benefits.[12] Unfortunately, even if open

[9] Strengthening Australia's Cybersecurity Regulations and Incentives, September 2021, Oceania Cybersecurity Centre, 25.
[10] Strengthening Australia's Cybersecurity Regulations and Incentives, September 2021, Oceania Cybersecurity Centre, 25.
[11] Strengthening Australia's Cybersecurity Regulations and Incentives, September 2021, Oceania Cybersecurity Centre, 25.
[12] Marcel Boer, 'Open-Source Data Platforms', *Medium* (Website, 24 May 2020), <https://medium.com/swlh/open-source-data-platforms-b3b4768f9e3e>.

data is first published as non-sensitive information, it could be matched with open data from other sources to start revealing sensitive information about a person.[13]

Question 1(c)

Should the obligations of company directors specifically address cybersecurity risks and consequences?

It is our submission that the duties (or obligations) of company directors should specifically address cybersecurity risks and consequences through mandatory penalties, with the insertion of direct, personal liability for such breaches similar to section 588G of the *Corporations Act 2001* (Cth).

The Potential Use of 'Stepping-Stone' Liability

A recent trend has emerged to keep company directors accountable, named the 'stepping-stone' approach, used mostly by ASIC. The approach has two stepping-stones; the first is finding that a company has contravened a section (or sections) of the *Corporations Act 2001* (Cth) ('*Corporations Act*') or another regime. The second stepping stone is a finding that due to the first contravention (or contraventions), the director exposed the company to the risk of criminal prosecution, civil liability or significant reputational damage, which is a breach of their general duty of care in section 180(1) of the *Corporations Act*.[14]

The term 'stepping-stone' approach was first coined in *Australian Securities and Investments Commission v Fortescue Metals Group Ltd* by Keane CJ.[15] The stepping-stone approach is perceived as a controversial application of the law because ASIC has used sections in the *Corporations Act* which do not impose a civil penalty liability as a stepping stone for section 180(1), which does impose this sanction.[16] The positive aspect of the stepping-stone approach is that it keeps company directors accountable for their decisions and awake to the current issues which may affect their shareholders, staff, and customers; risks such as cybersecurity breaches. This approach also does not require the creation of a specific individual duty in relation to areas of law (such as cyber risk), but allows that risk to be addressed in other

[13] Hacken, 'How sensitive is your non-sensitive data', *Hacken* (Website, 31 October 2018) <https://hacken.io/discover/how-sensitive-is-your-non-sensitive-data/>.
[14] Abe Herzberg and Helen Anderson 'Stepping Stones – From Corporate Fault to Directors' Personal Civil Liability' (2012) 40(2) *Federal Law Review* 181, 181.
[15] [2011] FCAFC 19, 10.
[16] Ian Ramsay and Miranda Webster 'An Analysis Of The Use Of Stepping-stones Liability Against Company Directors and Officers' (2021) 50(1) *Australian Bar Review* 168, 175.

legislation. A regulator (or other litigant) can step back to section 180(1) and argue that by permitting the company to breach the other legislative provision (which is significantly broader than requiring the breach to be committed by the director/s), the directors have also breached their duty of care.

Greenwood J's comments in *Cassimatis v Australian Securities and Investments Commission* rightly described the nature of s180(1) as normative, adding:

> Its burden is a matter of public concern not just private rights. It is an expression of the Parliament's intention to establish an objective normative standard of the degree of care and diligence directors must attain or discharge in exercising a power conferred on them or discharging a duty to be discharged by them.[17]

The stepping-stone approach used by ASIC highlights and solidifies the duty which directors accept when they undertake to act in the position as a company director. The stepping-stone approach could also be viewed as two separate prosecutions knitted together in one trial; the first stepping-stone, a contravention of the Act, becomes evidence for the second stepping-stone, the contravention of the directors' duties. Although, there is much more benefit in presenting the two prosecutions together because as Greenwood J held, directors are not found to have contravened section 180(1) of the *Corporations Act* because the company contravened another section of the *Corporations Act* (or other regime). The contravention of the directors' duty of care (codified in s 180(1)) is 'a necessary element of the harm' in contravening the first stepping-stone. This enlivens the notion that the first stepping-stone only occurred due to the breach of a duty of care. If a breach of duty occurs, director accountability will likely be sought in other ways regardless of whether ASIC uses the stepping-stone approach or not, by shareholders in a derivative action[18] or via the oppression remedy,[19] for example.

The interpretation of section 180(1) of the *Corporations Act* was broadened in the stepping-stone case of *Cassimatis*.[20] Edelman J commented that the foreseeable risk of harm to the corporation includes *all the interests of the corporation*, including reputation and compliance

---

[17] *Australian Securities and Investments Commission v Cassimatis* ('*Cassimatis'*) [2020] FCAFC 52, 27 (Greenwood J).
[18] *Corporations Act 2001* (Cth), s 236.
[19] *Corporations Act 2001* (Cth), s 232.
[20] Ian Ramsay and Miranda Webster 'An Analysis Of The Use Of Stepping-stones Liability Against Company Directors and Officers' (2021) 50(1) *Australian Bar Review* 168, 172.

with the law.[21] The statement suggests that a cybersecurity breach could be used as a stepping-stone to also prosecute under section 180(1) of the *Corporations Act*, because in most instances, a cyber breach exposes the company to both non-compliance with the law and reputational damage.

To date, ASIC has had a 72% success rate of its stepping-stones approach and the cases which have been unsuccessful were only due to the fact that they failed to prove the first contravention.[22] The Australian Institute of Company Directors ('AICD') has argued that an 'honest and reasonable director defence' should be included in the *Corporations Act* for additional director protections.[23] AICD has failed to clearly articulate why the existing business judgment rule (codified in section 180(2) of the *Corporations Act*) is insufficient. Whilst there is yet to be a successful implementation of the business judgment rule since its implementation in practice, it should still provide the same effect that AICD is seeking. Implementing an honest and reasonable defence would be far too generous of a protection and entirely unnecessary due to the existing business judgment rule. The stepping-stone approach will only capture those who are found to be negligent in the first instance. Directors who are not as active as they should be, or who do not seek advice from subject matter experts (i.e., cybersecurity and information technology experts) should be penalised, because not they are exposing the company to unacceptable risk, with the damage extending to their customers, staff, and shareholders.

Acceptance of Cyber Security Duties for Financial Services Licence Holders

In *ASIC v RI Advice Group Pty Ltd* ('*ASIC v RI Advice*')[24], RI Advice were found to have breached sections 912A(1)(a) ('do all things necessary to ensure that the financial services covered by the licence are provided efficiently, honestly and fairly') and 912A(1)(h) ('have adequate risk management systems') of the *Corporations Act* for failing to have adequate cybersecurity measures implemented across their representatives and failing to implement cybersecurity and cyber resilience measures which exposed their clients to an unacceptable level of risk. The sections above are specific obligations owed by holders of financial services

[21] Australian Securities and Investments Commission v Cassimatis [No 8], 483.
[22] Ian Ramsay and Miranda Webster 'An Analysis of The Use Of Stepping-stones Liability Against Company Directors' and Officers' (2021) 50(1) *Australian Bar Review* 168, 169.
[23] Australian Institute of Company Directors ('AICD'), The Honest and Reasonable Director Defence: A Proposal for Reform (Policy Paper, 7 August 2014) <http://www.companydirectors.com.au/Director-Resource-Centre/Policy-on-director-issues/Policy-Papers/2014/The-Honest-and-Reasonable-Director-Defence>.
[24] [2022] FCA 496.

licences and consequently are not transferable to the duties owed by directors of non-financial services companies. However, the decision highlights expanding judicial expectations of how a reasonable director of a company which provides a service where cyber-risk is heightened should mitigate cyber risks. Rofe J commented:

> Cybersecurity risk forms a significant risk connected with the conduct of the business and provision of financial services. It is not possible to reduce cybersecurity risk to zero, but it is possible to materially reduce cybersecurity risk through adequate cybersecurity documentation and controls to an acceptable level.[25]

ASIC v RI Advice confirms that cybersecurity responsibilities fall within financial services licensee's obligations, which are, admittedly, more specific than the general duty of care imposed on directors of non-financial-services corporations. Although these duties may not currently be imposed more generally on directors of non-financial institutions, as cyber risk expands to become a headline concern for all types of company, perhaps the policy reasons for restricting this provision to financial services licensees should be reconsidered.

The Duty of Care and Diligence Applied to Cyber Security

A director who does not adequately respond to cybersecurity risks, and does not ensure that the company is cyber resilient, exposes the company to unnecessary risk. It is our submission that they should therefore be held to be in breach of their duty of care. In *Australian Securities and Investments Commission v Vines*[26] Mr Vines, as chief financial officer of GIO Group (an insurance company) was held to have breached his duty of care and diligence by failing to inform a number of relevant decision makers of the true potential effect of Hurricane Georges. The information about Hurricane Georges should have led Mr Vines to advise the decision makers that it was improbable to achieve the forecast $80 million profit for GIO Re, the company within GIO Group which handled reinsurance at the time. Although there is not yet authority on point, the same argument can be attributed to cyber risk, whereby if a director or officer is aware of significant cyber risks and associated impacts and fails to address said risk, they should be found to have breached their duty of care.[27] Characteristics which are particularly relevant to courts in deciding duty of care and diligence cases appear to be whether

[25] Ibid, [58].
[26] (2005) 55 ACSR 617.
[27] A similar argument was made in relation to climate change risk using *ASIC v Vines* in Beth Nosworthy, 'The Corporations Act and Climate Change – Appetite for Change?' (2020) 94 *Australian Law Journal* 411, 414.

the breach was preventable, and whether the company and directors were 1) made aware of the risk prior to the incident and 2) whether they responded judiciously and in a timely manner. If a company is victim to cybercrime, not because of the directors' negligence, ignorance, or avoidance, the court will see the company, and the directors, as victims of a crime.

Personal Liability of Directors

Mandatory director penalties should be implemented for exposing the company to an unacceptable level of risk for a cybersecurity breach and/or for not having a cyber resilient company. In contrast to the mandatory penalties, adequate support for a company to ensure they are cyber resilient is required from government. Tax and financial incentives have also been suggested for cyber resilient organisations by the ATO.[28] Section 588G of the *Corporations Act 2001* (Cth) aims to prevent insolvent trading by holding directors personally accountable. The law regulating insolvent trading involves complex legal and accounting issues, just as cybersecurity requires significant IT expertise. According to ASIC, illegal phoenix activity, which involves one facet of insolvent trading, costs 'employees between $31 and $298 million in unpaid entitlements and costs the Government around $1.6 billion in unpaid taxes and compliance'.[29] In comparison, cybersecurity risk is significantly more expensive, costing $29 billion per annum to Australian businesses, and about $7 trillion worldwide.[30] These figures suggest that, measured by fiscal terms alone, cyber risk holds sufficient weight such that personal liability should be attached to a director who is operating a company with unsafe cyber measures. As unmitigated cyber risk has significant non-fiscal impacts on individuals whose data is breached, adding weight to the argument that cyber risk should become a personal liability for directors who fail to address it appropriately.

Whilst the duty of care and diligence owed by company directors under section 180(1) of the *Corporations Act 2001* (Cth) is agile enough to capture a wide range of directors who lack engagement in addressing cybersecurity risks, harsher penalties need to be implemented due to the rapidly growing consequences of cybercrime to individuals.

---

[28] https://www.ato.gov.au/General/New-legislation/In-detail/Direct-taxes/Income-tax-for-businesses/Small-Business-Technology-Investment-Boost-and-Small-Business-Skills-and-Training-Boost/
[29] https://asic.gov.au/for-business/small-business/closing-a-small-business/illegal-phoenix-activity/
[30] https://www.pwc.com.au/about-us/insights/non-executive-directors/cyber-security-director-responsibilities-in-a-changing-legislative-environment.html

Additional Protections

Industry and individuals must have a very clear understanding of their obligations and rights when dealing with data. Education on what data to collect, hold and dispose of (safely) is also required. The Australian Information Commissioner and Privacy Commissioner Angelene Falk said 'collecting the minimum amount of personal information required and deleting it when it is no longer needed' is an appropriate and proactive step for organisations to protect themselves against cyber threats.[31]

There is also scope to strengthen reporting obligations of companies who have experienced significant data breaches. Under the Notifiable Data Breach (NBD) scheme, an eligible data breach occurs when there is a 'serious risk of harm' to the affected individuals.[32] The problem is that the company conducts its own review in deciding whether a 'serious risk of harm' has resulted from their data breach, and whether disclosure is necessary. Recent data from the OIAC shows that two data breaches in 2020-2021, affecting more than 10 million people worldwide, still remain anonymous.[33] Not only is this an issue from prosecution and public scrutiny perspectives, the specific data that was stolen is still not known.[34] This is a problem, due to the 'mosaic effect' which explains that if one piece of data is exposed in a data breach, this might not say much about an individual, however, when brought together with other data that is publicly available about that individual it tells a much broader story, and can increase the risk of harm to that individual.[35] However, there is no expectation that a company should be held responsible for the mosaic effect, it just makes it particularly hard to assess the risk an individual is facing.

Every cyber breach that exposes data about several individuals should be made public, so that individuals can assess the risk they are facing. At present, companies are only required to report

---

[31] https://www.oaic.gov.au/newsroom/cyber-security-incidents-impact-data-breach-risk
[32] https://www.oaic.gov.au/privacy/notifiable-data-breaches/when-to-report-a-data-breach
[33] Julian Fell et al, 'This is the most detailed portrait yet of data breaches in Australia', *ABC News (online,* 28 March 2023) <https://www.abc.net.au/news/2023-03-28/detailed-portrait-data-breaches-oaic-disclosures/102131586>.
[34] Julian Fell et al, 'This is the most detailed portrait yet of data breaches in Australia', *ABC News (online,* 28 March 2023)< https://www.abc.net.au/news/2023-03-28/detailed-portrait-data-breaches-oaic-disclosures/102131586>.
[35] Julian Fell et al, 'This is the most detailed portrait yet of data breaches in Australia', *ABC News (online,* 28 March 2023)< https://www.abc.net.au/news/2023-03-28/detailed-portrait-data-breaches-oaic-disclosures/102131586>.

data breaches that pose a 'significant threat'.[36] Minor amounts of data can be knitted together (in the so-called mosaic approach) to tell a wider story about an individual, with significant detrimental consequences in terms of privacy, identity theft, fraud, and ultimately consumer confidence.

Conclusion

The intersection between cybersecurity law, company obligations and director duties are complicated. This is due to the several regulators who can potentially bring actions, such as ASIC under the *Corporations Act* and the Office of the Australian Information Commissioner' ('OAIC'), under the *Privacy Act 1988* (Cth) ('*Privacy Act*'). Class actions are also becoming increasingly prevalent, recently demonstrated by the Optus and Medibank breaches.

The overarching problem in Australia is that citizens are still not fully informed or aware of how valuable their data is, particularly for cyber criminals. Whilst the every-day person might find the spam text messages, emails and calls frustrating, the serious risk of harm they face with their data being leaked by an organisation is still not clearly understood. Organisations have the resources to understand this risk, and protect their customers accordingly. Therefore, stronger director and company obligations must exist in this power dynamic to protect the data-owners from serious cybercrimes. Companies should not have the privilege of accessing customer's data, profiting from the data via valuable analytics, and then exposing it to cybersecurity breaches due to a lack of diligence around cyber risk. Harsher penalties for company directors are required to protect individuals.

[36] Julian Fell et al, 'This is the most detailed portrait yet of data breaches in Australia', *ABC News (online,* 28 March 2023)< https://www.abc.net.au/news/2023-03-28/detailed-portrait-data-breaches-oaic-disclosures/102131586>.