Australian Institute of Company Directors

18 Jamison Street,
Sydney NSW 2000

t: 1300 739 119
e: contact@aicd.com.au
aicd.com.au

ABN 11 008 484 197

27 August 2021

Cyber, Digital and Technology Division
Department of Home Affairs

via email: techpolicy@homeaffairs.gov.au

Dear Department of Home Affairs

Strengthening Australia's cyber security regulation and incentives

Thank you for the opportunity to provide a submission in response to the Government's discussion paper, *Strengthening Australia's cyber security regulation and incentives* (**Discussion Paper**).

The Australian Institute of Company Directors' (**AICD**) mission is to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. The AICD's membership reflects the diversity of Australia's director community, our membership of more than 46,000 is drawn from directors and leaders of not-for-profits, large and small businesses and the government sector.

The AICD welcomes the Government's consultation on measures to strengthen cyber security and resilience, including governance and accountability practices across Australian businesses.

Australian directors are increasingly focused on the governance of cyber risk given the rapidly changing threat landscape and the increasing prevalence of attacks. The AICD's latest Director Sentiment Index for the first half of 2021 indicated that the percentage of directors nominating cyber-crime as an issue has increased to the second highest issue 'keeping directors awake at night.'[1]

Our submission focuses principally on areas of the Discussion Paper relating to options for strengthening governance standards (Section 1). Section 2 provides comments on the current regulatory framework and additional information for the Department of Home Affairs on Australia's unique director liability environment. Section 3 includes some brief comments on legal remedies for consumers, and Section 4 concludes with some observations on ransomware.

Executive Summary

The AICD is supportive of measures to strengthen cyber security and resilience, including governance and accountability practices across Australian businesses. The AICD's view is that a genuine partnership between government and industry has the best opportunity to result in significant improvements in cyber resilience across organisations of all sizes.

The AICD also encourages consideration of the various sectoral and jurisdictional obligations applying on cyber governance, which add complexity to the regulatory landscape and do not operate as a

[1] AICD Director Sentiment Index (April 2021), accessible here. This ranked equal with the disruption from COVID-19, and ahead of global uncertainty and climate change risks. Data security also saw a significant increase in rankings, moving from the 7th ranking to 3rd, behind cyber and COVID-19.

harmonised framework. Guidance for boards on cyber security obligations and good practice approaches would, in the AICD's view, be a more effective way to achieve the policy objectives outlined than regulatory standards.

Section 1: Governance standards for large business (Chapter 4 of the Discussion Paper)

- **Mandatory standard**: The AICD does not support the introduction of a mandatory cyber security governance standard. Existing directors' duties include an obligation to act with due care and diligence and this obligation appropriately covers emerging risks, such as cyber security. A mandatory standard would be a costly additional regulatory burden that may do little to improve cyber resilience but rather add to the existing complex patchwork of requirements that face large businesses in Australia.

- **Voluntary standard**: The AICD supports in-principle a voluntary standard co-designed with industry that focuses on conveying fit-for-purpose guidance in a non-prescriptive manner. For a voluntary standard to drive genuine benefits, it should be principles based and preserve organisational flexibility to respond dynamically to the evolving nature of cyber security risk. Importantly, the standard should avoid overlap, replication or conflict with existing obligations and requirements. Further consultation is required to consider key threshold issues, including scope, regulatory oversight accountability, the definition of 'large business' and which organisation has ownership and oversight of the standard.

- **Enhanced support from governments:** The AICD's consultation with directors has demonstrated significant demand for pathways to connect organisations with government advice, guidance and support, including when facing a live cyber incident. Governments, including state and federal law enforcement agencies, have an opportunity to collaborate with industry to improve tailored support and strengthen national resilience to cyber risks. A partnership approach would cover training, emerging threat intelligence, good practice guidance and pathways to law enforcement responses in the event of cyber security threats and incidents.

Section 2: Existing legal framework and the director liability environment (Chapter 3 of the Discussion Paper)

- **Directors' duties:** Existing directors' duties and other accountability obligations under the *Corporations Act 2001* (Cth) (**Corporations Act**) impose positive duties on directors to manage business risks including evolving risks such as cyber security.

- **Liability environment for Australian directors:** Australia's director liability environment is unique – and in many regards, uniquely burdensome – as compared with other jurisdictions. The AICD strongly cautions against the imposition of individual liability on specific or emerging risk issues when existing directors' duties already create a high standard of governance obligations. It is critical that policy settings are proportionate and avoid unnecessary complexity and regulatory burden. The focus should, instead, be on charting a path to national cyber resilience through co-designed best practice guidance.

Section 3: Protecting consumers (Chapter 10 of the Discussion Paper)

- **Clear legal remedies for consumers:** Cyber security incidents may be the result of malicious criminal or state actor activity and even companies with advanced cyber security protections can find themselves the victim of a cyber-attack. The AICD cautions against any approach that

would see entities and their officers 're-victimised' by being subject to actions (including potential class actions) where they have acted with honesty, integrity and diligence in their oversight of cyber security and data protection. We note that there are already rights of action for privacy breaches of this nature via common law or equitable actions.

Section 4: Additional considerations

- **Ransomware:** Although outside the scope of the discussion paper, the AICD recognises the escalating risk of ransomware attacks in the Australian cyber security landscape. The policy objective across regulatory, support and law enforcement initiatives should be to make Australia one of the least attractive jurisdictions to target for threat actors. In our view, this requires a greater focus on a partnership between industry and government to strengthen national resilience rather than focus on individual corporate liability settings. AICD feedback from directors across sectors suggests that companies and their directors would benefit from greater support as well as a clear path to law enforcement responses and expert governance expertise when faced with threats such as ransomware attacks. The AICD also encourages government to consider consultation on mechanisms to address the range of potential legal liability risks for directors associated with consideration of the payment of ransoms, and would be pleased to participate with member directors in this process.

- **Cyber insurance:** The AICD notes the critical role that insurers play, and the expertise that is often sourced through their networks, in supporting organisations when faced with a cyber-attack. The AICD recommends that government engage further with both industry and insurers on this complex issue.

Section 1: Governance standards for large businesses

The AICD does not support the introduction of a mandatory cyber security governance standard. As set out below, existing directors' duties establish clear governance obligations to effectively address emerging risks, such as cyber security. A compulsory standard would unnecessarily overlap with existing obligations and add to existing regulatory complexity to the challenges faced by boards in addressing this evolving risk.

The AICD supports in-principle a voluntary standard co-designed with industry. For any voluntary standard to drive change it should be in partnership with greater government support for organisations of all sizes, including consideration of good practice guidance.

Mandatory governance standards for larger businesses (Option 2)

We agree with the preliminary conclusion in the Discussion Paper that a mandatory standard would be too costly and onerous, particularly in an environment of significant regulatory change and where boards and organisations are actively taking steps to address this evolving risk.

The AICD acknowledges the growing and evolving nature of cyber security threats and the significant cost that cyber incidents place on businesses, individuals and the Australian economy as a whole. However, the AICD does not agree with the position in the Discussion Paper that organisations are not being incentivised to make the necessary security investments as the costs of any incident are borne by other market participants.

Feedback from our members and the results of a recent AICD survey of members shows that cyber security is prominent for most boards and organisations are seeking to comprehend the risks and to make investments to improve cyber resilience.[2] The AICD's member survey found a high proportion of respondents have taken a range of direct steps to improve organisational cyber resilience from engaging external experts to advise the board (58%) to embedding cyber security in existing risk management frameworks (75%). The survey results are consistent with feedback from AICD advisory committees and consultation with members across states and territories on this issue:

- cyber resilience is a priority issue for boards and organisations with corresponding investments in infrastructure and systems;
- greater engagement and collaboration with government is needed to support organisations, particularly small and medium sized, to enhance their cyber security maturity; and
- a voluntary standard would preserve flexibility for organisations to take specific targeted steps appropriate for their organisations to respond to a fast-moving risk.

This focus at the board level aligns with ASIC's observations of improvements in cyber resilience across financial services organisations of all sizes.[3] Rather than being indifferent to negative externalities resulting from a cyber incident these organisations are actively seeking to protect their operations and reputations to the benefit of stakeholders and customers. Notwithstanding this heightened focus, the increasing sophistication and complexity of cyber incidents, including the participation of state sponsored actors, presents significant challenges for organisations of all sizes.

In light of the heightened focus on cyber resilience by boards, and noting the application of core directors' duties, we are strongly of the view that a mandatory governance standard could be counterproductive and difficult to implement. We are concerned that a mandatory code would add to regulatory cost, and existing complexity, with limited potential benefit.

Many large businesses already are subject, or will be in the future, to a patchwork of existing cyber security requirements at both the Commonwealth and state government levels. The proposed amendments to the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**) represent a material expansion of the obligations on businesses in many key sectors of the Australian economy. Further, in 2019 the new APRA Prudential Standard CPS 234 Information Security (**CPS 234**) commenced and was applied to all APRA regulated entities. The Discussion Paper notes that approximately one third of ASX 200 companies are covered by industry specific security standards or requirements.[4] As well as industry-based requirements, organisations across the economy meet requirements under *Privacy Act 1988* (Cth) (**Privacy Act**), notably the Notifiable Data Breaches scheme and expectations for meeting Australian Privacy Principle 11 - Security of personal information.

We have received feedback that organisations already struggle with the complexity of meeting the existing requirements and preparing for new obligations. In addition, certain organisations, such as businesses with overseas operations or key international suppliers/customers, meet obligations in overseas jurisdictions and/or standards under the ISO 27000 series or the National Institute of Standards in Technology (**NIST**) Cybersecurity Framework.

2 AICD Cyber Survey was conducted between 29 July 2021 and 12 August 2021 covering 12 questions. Sample size was 266 directors drawn from public listed entities, private listed entities, public sector/government and not-for-profit entities.

3 ASIC, Cyber resilience of firms in Australia's financial markets: 2018–19, December 2019, page 3.

4 Discussion Paper, Strengthening Australia's cyber security regulations and incentives, 13 July 2021, page 13.

A new compulsory standard would add to the compliance burden of many organisations in an environment where many large businesses are grappling with regulatory change. Rather than drive genuine behavioural change in the management of this risk, including dynamic approaches, there is a likelihood that a compulsory standard would be become a compliance focused exercise. This would be exacerbated by uncertainty as to how any standard would be regulated and which regulator would have responsibility, as recognised by the Discussion Paper.[5]

Voluntary governance standards for larger businesses (Option 1)

While the AICD does not agree there are widespread market failures, we are supportive in principle of a voluntary standard, particularly if it is drafted as a standard to highlight good practice. A key objective of any standard, in conjunction with enhanced government support, would be to build cyber resilience to a level where Australian businesses are not perceived as attractive targets for sophisticated cyber-attacks.

To produce benefits that exceed the status quo (**Option – 0**) a voluntary standard would be co-developed with industry and be fit-for-purpose through preserving the flexibility of organisations to respond to evolving risks in a dynamic manner. The AICD considers that to maximise any benefit a voluntary standard would be accompanied by a strengthened partnership with t governments and enhanced support in key areas, as discussed below.

We strongly support a partnership between government and industry if a voluntary standard is pursued. A partnership approach will assist in the standard reflecting good practice, being practical to implement and appropriately recognising governance roles and responsibilities. A voluntary standard would ideally incorporate or link with guidance that already exists for large businesses, including publications by the Australian Cyber Security Centre (**ACSC**) and Australian Securities and Investments Commission (**ASIC**), and enable dynamic responses to evolving threats across the broader economy.

We appreciate the consultation on any governance standard is in the early stages, however we are concerned about the limited detail on the application and scope of a voluntary standard. For instance, it is not clear whether the standard would apply at the organisational/entity level or at the board or director level. We would expect that the standard would reflect on the existing directors' duties under section 180 of the Corporations Act and provide clarity to directors on how to approach these duties as they apply to cyber security.

A further threshold issue is which organisation or body would have ownership and oversight of the voluntary standard. It is not clear which government body would be the most appropriate home for oversight, or whether a co-regulatory model is proposed.

In addition to these threshold issues, for the standard to drive improvements in cyber resilience, then the following would be key features:

- principles-based drafting that reflects good governance practice, preserves organisational flexibility and avoids technical and operational specifications that would run the risk of becoming redundant as technology and the risk evolves;

[5] Ibid, page 22.

- no overlap with, or replication of, existing or pending Australian regulatory requirements, including the SOCI Act, CPS 234 and the Privacy Act. A principles-based standard would allow businesses discretion and flexibility to implement good practice consistent with their size, complexity, risk profile and industry rather than seek to impose obligations that exist in other frameworks and would not be fit-for-purpose across a diverse range of organisations;
- a robust definition of 'large business' that captures the right organisations;
- consideration of key international standards frameworks, including the ISO 27000 series and NIST; and
- practical reporting and audit expectations that incentivise self-assessment, continuous improvement and avoid counterproductive disclosure that promotes a checklist or compliance focused approach to meeting good practice under the standard.

A voluntary standard should be reviewed regularly to ensure it remains fit for purpose given the constantly evolving nature of cyber security risk.

The AICD strongly supports further work and cross-sectoral consultation on the development of a voluntary standard. The AICD would welcome the opportunity to contribute to any voluntary standard development process.

Definition of 'large business'

The ACID considers that the definition of 'large business' requires careful consideration to ensure the right organisations are captured under the voluntary standard.

The ACID supports in most policy initiatives utilising or aligning to existing definitions where possible as a method for reducing complexity and compliance costs. However, in this instance existing frameworks may not appropriately reflect the business models and practices of organisations that are key to cyber security in Australia.

Feedback from members on the AICD Reporting Committee has noted the shortfalls of adopting an existing framework. Traditional measures of size, such as annual turnover or number of assets, may not be characteristics of entities that hold personal or sensitive data or provide goods and services relevant to cyber security or information systems more generally. For this reason, adoption of existing legislative thresholds in other regulatory regimes may not be appropriate.

The AICD recognises the challenges in developing accurate and measurable thresholds to capture the right large businesses and organisations. The AICD would be happy to contribute to consultation on definitions as a component of the broader development of a voluntary standard, including engaging with the AICD Reporting Committee.

Enhanced government support

The AICD considers that for any voluntary standard to be effective in lifting practices it must be in partnership with enhanced government support and further opportunities for collaboration. This support would encompass training, best practice material and government resources and assistance to understand and respond to emerging threats and risks.

The AICD recognises the significant investment by the government in cyber security skills via the Cyber Security Skills Partnership Innovation Fund. As found by the 2021 joint report by RMIT Online and Deloitte Access Economic Australia faces a significant gap in digital skills across its workforce.[6]

We note that the AICD is also lifting its focus on the governance of cyber risks and is committed to building the capability of directors and boards to tackle the rapidly changing cyber-threat landscape. The AICD offers a number of formal training opportunities for company directors on cyber security risk management. This includes a new course offering, *The Board's Role in Cyber*, which has had significant demand from members and an online micro-course with over 1,200 members having registered since launch in June 2021. Cyber security also features regularly in AICD member content and the AICD's new Digital Directors podcast.

The AICD also strongly supports enhanced government and industry collaboration to boost cyber governance and national resilience. This support would encompass training, best practice material and resources and assistance to understand emerging threats and risks.

Our survey of AICD members revealed demand for additional support with 79% of respondents seeking further education and training, 57% seeking sector specific best practice guidance and 56% seeing the need for genuine partnerships between law enforcement and intelligence agencies. While organisations and directors are rightly expected to continue to educate and inform themselves on cyber risks there is a key role for government as a trusted source in supporting these activities.

The AICD does not have direct comment on the Discussion Paper options in respect of health checks for small businesses. However, feedback from members is that additional training and support targeted at small and medium sized enterprises (**SMEs**) would likely produce a greater benefit than health checks. As reflected in the consultation paper SMEs have limited time, resources and existing cyber expertise with resulting gaps in cyber resilience.[7] The SME initiatives funded under Australia's Cyber Security Strategy 2020 represent important steps in addressing gaps. However, there may be room for additional targeted training and support initiatives, including for directors of SMEs, that would further assist in narrowing these gaps.

The ACSC produces a large volume of guidance for different sized organisations and individuals. However there does appear to be a gap with translating existing guidance into a coherent set of expectations for boards and directors, in a good practice guidance model. Forty-six per cent of respondents to the survey noted a lack of clarity around what is better practice as a key barrier to adopting stronger cyber security practices. A well-structured voluntary standard represents an opportunity to elevate existing governance good practice and compliment it with further guidance. Importantly these resources could be directed at not just large businesses subject to the standard but also SMEs.

In addition to opportunities for training and guidance, our members consider there is scope for additional collaboration with government on emerging threats and risks. This could take the form of intelligence and assistance from government and law enforcement agencies on current incidents or threats and expert advice where necessary. While large well-resourced businesses can access third party experts in the event of a cyber security incident this is not available to many organisations. The government as a trusted source of support and intelligence could play a key role in closing this information gap. This type of cooperative engagement could assist organisations and directors

[6] See New report reveals Australia's major digital skills gap - RMIT University, 9 February 2021

[7] Discussion Paper, Strengthening Australia's cyber security regulations and incentives, 13 July 2021, p.47

enhance their knowledge of how to defend and respond to cyber incidents and strengthen the principles-based guidance in the voluntary standard.

We recommend further engagement with industry on what support the government may provide to support cyber resilience in conjunction with work on a voluntary standard.

AICD position

The AICD supports in-principle a co-designed voluntary standard and recommends further engagement with industry on the scope and key features of any standard. To be effective at supporting cyber governance practices we recommend that a voluntary standard is accompanied by additional government support and collaboration.

Section 2: The current regulatory framework and other relevant information

The AICD agrees with the Discussion Paper that there is an opportunity to use Australia's existing legal and regulatory framework to create stronger incentives for Australian businesses to invest in cyber security resilience. However, in doing so, it is critical to get the policy settings right and avoid unnecessary regulatory burden.

The AICD is pleased to see the Government's proposals do not contemplate imposing specific legislative duties and additional director liability, given the potential for duplication of existing director obligations and the nature of the existing liability environment for Australian directors. We strongly caution against this form of regulation whenever there is a new emerging issue to be addressed.

Directors' duties

The AICD does not consider that Australia's corporations laws and directors' duties are limited in clarity and coverage in effectively addressing cyber security threats, or are solely focused on protecting the interests of shareholders, rather than customers and other stakeholders. In our view, ensuring cyber security resilience forms part of many existing obligations including those applicable to directors under both the common law and the Corporations Act.

As noted in the discussion paper, the Corporations Act laws that apply most relevantly to safeguarding against cyber security risks include:

- **Duty to act with care and diligence:** Sections 180 of the Corporations Act imposes a civil obligation in relation to care and diligence which requires directors to guard against key business risks. Importantly, there is no 'one-size-fits-all' approach to compliance with section 180. Directors must be able to demonstrate they have exercised a *reasonable* degree of care and diligence. In practice, this requires directors to stay informed and apply an enquiring mind about the organisation's activities, monitor the organisation's affairs and policies, test information put before them by management and proactively consider what other information they require. These obligations apply to a wide range of business risks, including having appropriate systems in place to ensure cyber security resilience as well as prevent and respond to cyber incidents.

- **Duty to act in good faith in the best interests of the company:** Section 181 of the Corporations Act requires directors to exercise their powers and discharge their duties in good faith in the best interests of the company, and for a proper purpose. It is increasingly recognised however that decisions made by a board will have an effect on an organisation's stakeholders beyond

its shareholders, including employees, customers, suppliers and the broader community. Recent court decisions in Australia have confirmed that the duty to act in the best interests of the organisation cannot be isolated from the interests of other stakeholders and directors have considerable latitude to factor stakeholder interests into decision-making.

It is important to note that there is also a nexus to these core directors' duties in the case of a breach of other Corporations Act provisions arises due to the operation of 'stepping stone liability', which is a unique feature of the Australian director liability environment. This form of direct liability involves a 'two-step process', whereby directors can be found personally liable for a breach of their directors' duties under the Corporations Act where an entity has failed to prevent contraventions of law or comply with its accountability obligations.[8] For directors to be liable, there must be some degree of involvement in the entity's breach such that it could be said the directors failed to exercise their duties properly and with due care and diligence.

As noted above, the proposed amendments to the SOCI Act will represent a material expansion of the obligations on businesses in many key sectors of the Australian economy. Directors of Australian Financial Services License (**AFSL**) holders are also subject to general and specific obligations under Chapter 7 of the Corporations Act. Specifically, section 912A(1) of the Corporations Act sets out a range of obligations for AFSL holders, including to have in place risk management systems and controls to manage business risks.

The Discussion Paper notes that ASIC has commenced its first enforcement action against an AFSL holder, RI Advice, under section 912A(1) for breaches arising from a failure to have adequate cyber security systems and a remediation plan for cyber incidents. The RI Advice action demonstrates that ASIC considers cyber risks as a key systems and control issue, and that cyber governance failures are within its investigatory remit. It is not yet clear whether ASIC will also pursue a breach of directors' duties action against the directors of RI Advice via the stepping stones liability. However, the outcome of these proceedings will provide judicial guidance not only about the cyber security standards required of AFSL holders, but also more generally the standard of care and diligence required of directors in the discharge of their duty under section 180 of the Corporations Act to guard against cyber security risks.

AICD position

In the AICD's view, irrespective of whether the Government decides to adopt a voluntary or mandatory governance standard, existing directors' duties and other accountability obligations on entities to manage business risks under the Corporations Act, including through the imposition of stepping stones liability, provides sufficient recourse both against entities and their directors for any failure to effectively address cyber security threats.

However, as the discussion paper highlights, should the Government opt for a voluntary governance standard, compliance with this framework may nonetheless become the high water-mark standard of care in civil proceedings or ASIC prosecutions for breaches of the directors' duties. Accordingly, in our view, there is an opportunity for a voluntary standard to complement existing directors' duties by providing best practice guidance for directors and organisations, without the imposition of duplicative obligations and liability.

[8] Jennifer Hill, 'Legal Personhood and Liability for Flawed Corporate Cultures' (European Corporate Governance Institute (ECGI)-Law Working Paper 431, 2018) 27.

Liability environment for Australian directors

It is important to also understand the liability backdrop against which Australian directors' duties operate in Australia.

The AICD commissioned law firm Allens to prepare two pieces of research comparing frameworks for imposing criminal and civil liability on directors in Australia and comparative jurisdictions (the UK, New Zealand, Canada, Hong Kong and the USA) and, separately, the operation of the business judgment rule. Allens concluded that Australia's director liability environment is unique - and in many regards, uniquely burdensome - as compared with other jurisdictions.[9]

In particular, key features identified included:

- **Business judgment rule:**
    - The liability risk for Australian directors is furthered by the lack of protection provided by the business judgment rule, contained in section 180(2) of the Corporations Act. The purpose of the business judgment rule is to protect the authority of directors to make bona fide commercial decisions, acknowledge that directors make decisions with imperfect information, and avoid an unreasonable level of risk aversion and encourage sensible commercial risk-taking.
    - Allens also notes that despite common policy objectives, Australia's business judgment rule operates differently, has never been successfully pleaded by a defendant director, has a narrower application and provides less protection to directors than comparator jurisdictions' business judgment rules.[10]
- **ASIC enforcement:** Australia relies on public enforcement of duties via ASIC, whereas comparator jurisdictions rely almost exclusively on private enforcement of directors' duties. This means that when overseas lawmakers and regulators are looking to impose new obligations or regimes, they do not have the same arsenal of public enforcement mechanisms and may need to create bespoke industry-specific ones.
- **Criminal liability imposed liberally:** Australia imposes criminal liability (with harsh penalties) on directors relatively liberally, particularly in relation to dishonest or reckless contraventions of their corporate governance obligations;
- **Harsh civil penalties:** Australia's civil penalties are harsh, even as compared with Australian and other jurisdiction's criminal pecuniary penalties.

Unintended consequences of additional liability

The AICD is of the view that directors should be held accountable for their direct governance obligations, with appropriate and proportionate penalties. This is, of course, a critical part of any successful framework for good corporate governance.

However, as noted in the Discussion Paper, cyber security incidents are increasing in frequency, scale and sophistication. The AICD's recent member survey on cyber security indicates the primary factors

[9] The full research paper is available here.

[10] The Allens report is available here.

preventing boards from adopting better cyber security practices within their organisations are due the nature of the threat evolving quicker than organisations can respond (46%) and the lack of clarity about what is better practice (46%). Imposing liability on directors, with public enforcement and serious consequences for breach, in circumstances where the extent of the obligation is constantly evolving and complex given the sophisticated threat actors (and often state actors) responsible for cyber incidents is, in our view, unreasonable and inappropriate.

It may also lead to an understandable board preoccupation with compliance and personal liability concerns over other responsibilities such as strategy, growth and innovation.

Section 3: Clear legal remedies for consumers

We understand that Government is contemplating providing stronger rights of recourse to compensate consumers for cyber security incidents. As noted in the Discussion Paper, this may include providing a direct right of action, via privacy class action claims or permitting the Office of the Australian Information Commissioner (**OAIC**) to bring proceedings on behalf of consumers, for privacy breaches where businesses have not taken reasonable steps to protect personal information.

Although this is being considered as part of the Privacy Act Review, the AICD would caution against any reform that may result in a proliferation of class actions for privacy breaches due to cyber security attacks. Depending on the circumstances of the incident, profile of the breached entity, and relationship with affected individuals, there are already rights of action for privacy breaches of this nature via common law or equitable actions, such as negligence, breach of contract, breach of confidence, misleading and deceptive conduct, or breach of continuous disclosure obligations.

Cyber security incidents may be the result of well-resourced malicious criminal or state actor activity and even companies that have best practice cyber security approaches can find themselves the victim of a cyber-attack. In our view, it would be unacceptable to have entities and their directors re-victimised by being subject to the further risk of a class action claim for a breach of privacy, or otherwise owing to a decision to pay or not pay a cyber ransom (discussed further below), where they have acted with honesty, integrity and diligence in their oversight of cyber security and data protection.

Section 4: Additional considerations

Ransomware

Although outside the scope of the Discussion Paper, we would note that an escalating risk in the Australian cyber security landscape is ransomware attacks and the range of potential legal liability risks associated with the payment of ransoms. These include potential exposure to 'instruments of crime' offences under *Criminal Code Act 1995* (Cth), liability under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*(Cth), as well as class action claims where a company's decision to pay, or not pay, a cyber ransom has an adverse material adverse impact on the company or the privacy rights of affected individuals.

Companies and their directors need greater support from government and law enforcement to ensure there is a clear path to support and expertise when faced with ransom demand. Feedback from the AICD's members is that ransomware attacks are an increasingly complex issue for organisations and that greater transparency around the prevalence of attacks in Australia, as well as what actions companies have taken in the aftermath, would be of assistance. We recommend that

government undertake further targeted engagement with industry on what support is needed in this area. The AICD would also support consultation with industry on more effective intelligence sharing on ransomware threats.

Cyber insurance

As part of the Government's consultation on strengthening governance standards and providing clear legal remedies for consumers affected by cyber security incidents, we support further consideration of the implications for cyber insurance. The AICD has heard from members of the critical role that insurers play, and the expertise that is often sourced through their network, in supporting organisations when faced with a ransom demand, particularly in the absence of clear paths to existing coordinated national resilience and response support.

The AICD does not consider that the withdrawal of cyber insurance is an appropriate mechanism to mitigate the risk of ransomware attacks occurring. This is a complex issue and we recommend that government further engage with both industry and insurers regarding the cost of, and access to, cyber insurance for organisations of every size in Australia. Insurance is a critical risk mitigation tool with the preservation of appropriate cover being crucial to attracting and retaining the most skilled and dedicated directors to Australian boards.

Next steps

We hope our response will be of assistance with this important consultation.

In our view, the development of any governance standard will benefit from engagement with directors. We would be pleased to facilitate access to the AICD's network of directors, advisory committees and experts on governance and boardroom practice. This might include, for example, facilitating targeted roundtables between the Department and directors to discuss the consultation options further and to help address identified challenges.

If you would like to discuss any aspects further, please contact Laura Bacon at lbacon@aicd.com.au or Simon Mitchell at smitchell@aicd.com.au.

Yours sincerely,

Louise Petschler GAICD
General Manager, Advocacy