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

14 April 2023

Department of Home Affairs

auscyberstrategy@homeaffairs.gov.au

Dear Advisory Board and Department of Home Affairs

2023-2030 Australian Cyber Security Strategy – Discussion Paper

Thank you for the opportunity to comment on the *2023-2030 Australian Cyber Security Strategy* (**Strategy**) Discussion Paper (**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 of 50,000 reflects the diversity of Australia's director community, comprised of directors and leaders of not-for-profits (**NFPs**), large and small and medium enterprises (**SMEs**) and the government sector.

The AICD has in recent years engaged extensively on Government consultations and proposed reforms in the cyber security and data management policy areas, including the Government's consultation on *Strengthening Australia's cyber security regulation and incentives,* the *Security of Critical Infrastructure Act 2018* (**SOCI Act**) and *Privacy Act 1988* (**Privacy Act**).

We have also sought to support our membership to improve their knowledge of cyber security best practice through extensive guidance materials and educational offerings, most notably the world first Cyber Security Governance Principles, developed in collaboration with the Cyber Security Cooperative Research Centre (discussed below).

Enclosed at **Attachment A** are our detailed responses to a number of key questions contained within the Discussion Paper. The AICD's policy positions have been informed by extensive engagement with cyber security and legal experts, entities, Australian businesses, industry bodies and the director community.

Executive Summary

The AICD strongly supports Government and industry working together to ensure that Australia is a world leader in cyber security with citizens having confidence that our economy operates within a secure and trusted digital environment.

A Government- industry partnership should focus on enhancing cyber resilience across the Australian economy with any new regulations being risk-based and developed with a strong appreciation of the potential compliance costs and impacts on innovation. There is a danger that introducing additional regulation, including at the board level, will result in a culture that prioritises being cyber compliant rather than cyber resilient.

Our key points on the topics in the Discussion Paper are as follows:

- Australia's existing corporations law and directors' duties provide a comprehensive and clear legal framework that obliges directors to effectively oversee the management of cyber security risk and build cyber security resilience. The AICD does not support introducing new cyber-specific director

duties. There is no shortage of existing legal obligations that create a strong incentive for appropriate cyber risk management. No comparable jurisdiction has imposed a cyber duty on directors, and the Australian director liability environment is already uniquely burdensome compared with peer jurisdictions. Similarly, we do not consider there is a convincing case for the development of mandatory cyber security standards given the existing patchwork of cyber-related regulatory regimes in Australia. Policy outcomes should be aimed at streamlining cyber-related obligations, not adding complexity.

- The AICD does not support further amendments to the SOCI Act in the short term. While, in-principle, we would not oppose an expanded definition of critical assets, our strong view is that the Government's priority should be on raising awareness of the SOCI Act obligations and conveying best practice expectations rather than pursuing further amendments at this time.

- The AICD in-principle supports a standalone Cyber Security Act that consolidates and harmonises existing cyber regulatory obligations under one legislative framework. We would not support a standalone Cyber Security Act that introduces new obligations on organisations and directors, layering additional regulatory requirements over existing regulatory structures.

- The AICD is not convinced that a strict legislative prohibition on the payment of ransoms and extortion demands by either victims or insurers is appropriate. Decisions in this area are extremely complex and can have far-reaching consequences beyond the entity itself. To avoid unintended outcomes, there is benefit in preserving a degree of flexibility so that entities, with the support of experts, determine the appropriateness of payment in the specific circumstances.

- The AICD supports the Government clarifying its position with respect to payment of ransoms and the circumstances in which this may constitute a breach of Australian law. We also consider there is a pivotal role for Government to play in providing enhanced guidance and support to entities in respect of ransomware and extortion demands.

- The AICD strongly supports explicit confidentiality obligations on the Australian Signals Directorate (**ASD**), and other key agencies as appropriate, in respect of information provided to it by organisations sharing cyber threat intelligence and notifying, and seeking assistance, in respect of a significant cyber incident.

- The AICD strongly supports the establishment of a single reporting portal for all cyber and data breach incidents. We also in-principle support all large businesses being required to notify ransomware and data extortion incidents.

Next Steps

We hope our submission will be of assistance. If you would like to discuss any aspects further, please contact Simon Mitchell, Senior Policy Adviser at [redacted], Laura Bacon, Senior Policy Adviser at [redacted] or Christian Gergis, Head of Policy, at [redacted].

Yours sincerely,

[redacted]

Louise Petschler GAICD
General Manager, Education & Policy Leadership

Attachment A: Responses to key questions

1. Director oversight of cyber security resilience

AICD members are highly engaged on the governance of cyber security and data protection and are motivated to build the cyber resilience of their organisations. Cyber-crime and data security has been over recent years consistently cited as the number one issue "keeping directors awake at night" in the AICD's biannual Director Sentiment Index (**DSI**).[1]

Consistent feedback from our members, who are on the boards of organisations of all sizes, is that they are focused on the significant damage a cyber security incident creates and the major financial, litigation and reputational risks that often flow from these events. The AICD's recent DSI results for the first half of 2023 indicate that 83% of directors are aware of their organisation's obligations related to the collection, storage and management of personal information. 69% of respondents also report that their board understands what personal or employee data is collected, who has access to it and where it is stored. Existing regulatory regimes, notably the Privacy Act, SOCI Act, APRA prudential standards and director duties under the *Corporations Act 2001 (Cth)* (**Corporations Act**), serve to strongly reinforce the importance of active board oversight.

The AICD would therefore resist the assumption, which appears implicit in the Discussion Paper, that existing legal obligations do not create a sufficient incentive for directors and senior leaders to appropriately manage cyber risks. In our view, in keeping with sound policy development principles, there needs to be a clear evidence base that suggests that new obligations are necessary or desirable.

We are not aware of any credible stakeholder that has put forward the view that directors are not *already* exposed to liability risk for poor cyber risk management practices, especially under section 180 of the Corporations Act (discussed further below).

What directors are seeking from the Government is coordinated policy making that is focused on industry support and assistance, and a partnership approach that facilitates sharing of information, response support and guidance on good practice.

AICD CSCRC Cyber Security Governance Principles

To support directors in governing cyber risk the AICD published the Cyber Security Governance Principles (**the Cyber Principles**), developed in partnership with the Cyber Security Cooperative Research Centre (**CSCRC**), in October 2022.[2]

The Cyber Principles have filled an identified gap in practical guidance available to Australian directors to effectively oversee and engage with management on this evolving risk. The Cyber Principles have received the endorsement of the Minister for Home Affairs and Cyber Security, the Hon Clare O'Neil MP, as well as ASIC Chair, Joe Longo.[3] To date, the Cyber Principles and supporting resources have received over 17,000 unique downloads reflecting the appetite of directors to improve their knowledge of cyber security risk and build organisational cyber resilience.

[1] AICD Director Sentiment Index, Second Half 2022, available here.
[2] AICD CSCRC Cyber Security Governance Principles, October 2022, available here.
[3] ASIC Chair's remarks at the AICD Australian Governance Summit 2023, available here.

The Cyber Principles are an example of how a collaborative approach can produce dynamic support and guidance that drives meaningful improvements in cyber security resilience across the economy.

Comparative review of cyber regulation globally

In February 2023 the AICD commissioned King & Wood Mallesons (**KWM**) to analyse comparable jurisdictions' cyber security regulatory settings. The objective of the analysis is to understand where Australia sits in comparison to peer jurisdictions, the United States, Canada, European Union and the United Kingdom (**UK**). The analysis (**Attachment B)** highlights key themes in the areas of board accountability and governance; sector-specific cyber security obligations; future directions in regulation; and international coordination and response to cyber incidents.

At a high level, the KWM analysis finds:

1. **No other comparator jurisdiction has imposed a general duty on directors** in relation to cyber security;

2. **Australia currently has some of the strongest cyber specific obligations on directors in respect of critical infrastructure or systems of national significance** when compared to other jurisdictions; and

3. There is **increasing scope for class actions** to be brought directly against directors arising out of a cyber security or data breach across all jurisdictions.

The analysis demonstrates that the international cyber regulatory landscape is evolving. However, each of the comparator jurisdictions share common cyber policy objectives to Australia and are implementing regulatory reforms in a way that is increasingly consistent. Given the global nature of cyber security risk, this 'lock step' approach is important.

In contrast, the scope and nature of proposals included in the Discussion Paper, most notably the proposed new cyber directors' duties and prohibition on ransom payments, extend beyond measures either in effect or being contemplated in overseas regimes.

Although strengthening economy-wide cyber resilience is a national issue, Australia's strategy must recognise cyber security is a global issue requiring a coordinated policy and regulatory approach across jurisdictions. We urge ongoing international collaboration in this area of policy-making to ensure Australia does not become a global outlier with unintended consequences.

2. Coordinated and partnership-based approach

2a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

The AICD supports a coordinated and partnership-based approach to improving cyber security practices and resilience across the economy, with further regulation being targeted and risk based.

In developing the Cyber Principles, and through engagement on earlier reform proposals, AICD members have expressed concern with a perceived lack of coordination on cyber security related reforms that span different policy portfolios.

An example is that Government is developing the critical *2023-230 Cyber Strategy* under the Home Affairs and Cyber portfolio, while also contemplating fundamental related changes to the Privacy Act under the Attorney General's portfolio. These two important initiatives are both focused on strengthening

Australian cyber security and data management practices, but are not necessarily aligned. This risks layering new regulatory obligations on top of an already highly complex privacy and cyber security landscape.

The Productivity Commission, in its recently concluded productivity inquiry, had a significant focus on digital and data settings in Australia, including balancing cyber security regulation and growth. Productivity Commission noted:

> *The government's role in mitigating and managing cyber risk is important, but can involve restrictions or additional requirements on private entities, which may inhibit economic growth. For example, unnecessarily burdensome regulation can divert businesses' resources away from other operations, which may negatively affect broader business activities or undermine existing security protocols.*[4]

The Productivity Commission found 'that Government initiatives to improve cyber resilience and response should be 'light touch' where the risks are relatively low'. Further, it considered that further cyber regulation should be targeted at high-risk areas:

> *More substantial government intervention could involve imposing regulation on companies for which an attack would represent a significant broader risk. Cyber security regulations must be designed implemented in a way that minimises unnecessary burdens, is not excessively intrusive and establishes clear expectations of the regulated entities.*[5]

The United States Government in its recently published *National Cybersecurity Strategy* also flags a rebalancing of the onus of cyber security obligations *away* from individuals and smaller organisations *towards* organisations that are best placed to reduce risks for the community.[6]

Informed by engagement with directors, the findings of the Productivity Commission and legal analysis of international settings, the AICD considers that a partnership approach to enhancing Australia's cyber resilience should comprise three core components:

	Component	Focus areas
1.	**Risk focused regulatory reform**	• Targeted enhancements to the SOCI Act • Reform of the Privacy Act • Ransomware reporting
2.	**Harmonisation and streamlining**	• Cyber Security Act as a mechanism to consolidate and streamline obligations • Single reporting portal
3	**Support and collaboration**	• Focused support for SMEs and NFPs • Enhanced intelligence sharing and collaboration between Government and industry

[4] Productivity Commission, Advancing Prosperity 5-year Productivity Inquiry Report, Volume 4: Australia's data and digital dividend, page 77.
5 Ibid, pages 78-79.
[6] The White House, National Cybersecurity Strategy, March 2023.

		• Targeted government investment in building Australia cyber security resilience

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?

a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?

The velocity of the cyber security threat and its relevance to all Australian organisations and individuals presents a challenge for the Government in improving cyber security best practice knowledge and behaviour.

The AICD considers there is an opportunity for a deeper partnership between Government and industry to raise awareness of cyber security threats and promote best practice. This partnership could be boosted by targeted investment by Government, including for research and development where appropriate.

We commend the existing level of guidance and resources provided by Government agencies on cyber security best practice. In particular, the Australian Cyber Security Centre (**ACSC**) develops and publishes a significant volume of guidance and alerts targeted at a wide range of audiences. Our view, informed by feedback from directors, is that there can be limited awareness of this guidance and the tools and assistance that Government can provide on cyber security to organisations across the community.

The strong director interest in the Cyber Principles indicates that in some instances industry bodies, or particular corporations (e.g. large banks or telecommunications providers), may have advantages in reaching key cohorts of businesses and individuals. The AICD and CSCRC benefited from feedback and input from key Government regulators during the development of the Cyber Principles. Our view is that this is an example of a model for how industry can work collaboratively with Government to provide targeted resources to lift cyber practices more generally.

The US Government's recently announced *National Cybersecurity Strategy* commits research and development investments from the Federal Government 'in defensible and resilient architectures and reduce vulnerabilities in underlying technologies'.[7] Similar targeted investments in Australia would help fortify key cyber security infrastructure and lift corporate cyber resilience. An investment approach focused on critical infrastructure would have benefits throughout the supply chain, including to SMEs and individuals. For example, this may comprise research and development support for critical asset owners focused on enhancements to key digital systems and infrastructure.

SMEs and NFPs

The AICD recommends that building the cyber security resilience of SMEs and NFPs be a priority area, as it is key to improving Australia's overall resilience.

A narrow focus on increased compliance and punitive measures that extend to SMEs and NFPs would be counterproductive and be unlikely to make any material difference to Australia's overall cyber posture.

[7] The White House, National Cybersecurity Strategy, March 2023, page 24.

The AICD's observation, based on feedback from directors and industry experts, is that there are significant challenges for SMEs and NFPs in addressing cyber security and data management risks. SME and NFP directors have noted that while they are alive to the cyber security risks their organisations face, they face considerable resource and time constraints in addressing these risks and very limited support from Government. This observation is consistent with the Productivity Commission's findings that small businesses are slower to take-up new digital tools, including cyber security software.[8]

In our recent submission to the Attorney General's Department consultation on the Privacy Act Review Final Report, we did not support the wholesale removal of the small business exemption.[9] The AICD considers that a targeted risk-based approach focused on the sectors where there are greater data and cyber risks would be a more effective policy intervention. The AICD is concerned that removing the small business exemption and imposing the full suite of Privacy Act obligations on all small businesses, would unduly increase regulatory costs and result in minimal compliance little benefit to cyber resilience.[10]

This AICD policy position extends to several cyber regulatory reforms in the Discussion Paper, including expanded reporting and notification requirements. Our view, as detailed below, is that these should be applied to large businesses that have the awareness and resources to meet them in a comprehensive manner.

We recommend the Government focus on lifting the cyber resilience and data management practices of SMEs and NFPs through targeted support, such as:

- *Expanded training and education programs*. We support the recently funded Cyber Security Business Connect and Protect Program and, dependent on evaluation results, encourage the Government to consider whether the program could be expanded to reach more participants;

- *Expanded ACSC guidance*. We support the ACSC continuing to develop specific guidance and materials for SMEs and NFPs. Our concern is that guidance may at times be "lost" in the volume of quality materials on the ACSC website. In our view, improvements could be made to the navigability of the ACSC website to ensure these materials are easily accessible by directors and managers of SMEs and NFPs. We note the approach in the UK where the National Cyber Security Centre has launched easy to use Free Cyber Action Plan and Check Your Security portals and interactive tools for small businesses and individuals. We encourage Government to look to trial examples of successful guidance and outreach between cyber agencies and small businesses as a priority

- *Assistance and advice in the event of a significant cyber incident* and in particular, ransomware attacks as discussed further below, for instance via a dedicated web portal or the ACSC hotline (currently used as a mechanism for reporting incidents only); and

- *Public information campaign*. A public information campaign focused on individuals and small businesses will assist in raising awareness, including where to seek guidance and support. For example, SME directors or owners may blur their personal cyber security settings with business settings, using one mobile phone. Public awareness messaging focused on low-cost changes (e.g. passphrase settings) may result in practical improvements.

[8] Productivity Commission, Advancing Prosperity 5-year Productivity Inquiry Report, Volume 4: Australia's data and digital dividend, page 22.
[9] AICD submission to the Privacy Act Review Final Report, available here.
[10] For instance, one example would be the requirement for all small businesses to have a nominated privacy officer.

12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

The AICD considers that Government measures to build the capability and depth of Australia's cyber security workforce will be key to strengthening Australia's cyber posture. In our view, there are a range of measures that Government can implement to bolster the strength of our cyber security expertise in Australia, including targeted skilled migration as an integral component.

We have received extensive feedback from members that organisations of all sizes have challenges in recruiting skilled and experience cyber security professionals. This is supported by research that indicates that there will be a shortfall of cyber security professionals of between 25,000 – 30,000 in Australia by 2024.[11]

The AICD strongly supports initiatives to support cyber security education and training via Australia's tertiary and vocational education systems. We also encourage the Government to not just limit its focus on cyber security education to formal degrees or courses via institutions. Targeted short training and education materials for those involved in the management and governance of organisations has the potential to deliver sizeable returns on investment. In particular, as discussed above, we see significant opportunity for the directors and managers of SMEs and NFPs to receive targeted support that focuses on practical and low-cost enhancements they can make to build cyber resilience.

We also see a role for industry associations and organisations to support cyber security education, for example we applaud the CyberCX Academy initiative. We note that over 1,600 members have undertaken the AICD's courses on cyber security since August 2020, including our most recent edition, *The Board's Role in Cyber*. 6,000 members have also participated in the AICD's *Digital Directors* webinar series focussed on emerging digital governance practices and funded by the Commonwealth Department of Industry, Science, Energy and Resources.

The AICD strongly supports the Government examining how targeted skilled migration can assist in meeting the cyber security skills gap. We have received consistent feedback from directors that lifting restrictions on skilled migration are fundamental to strengthening the talent gap across a range of industries in Australia, particularly technology and cyber security. Our view is that solutions in category-specific targeted migration should be pursued together with investment in domestic education and training initiatives. A long term, and sustainable approach needs to be taken.

The AICD also supports the Government assessing whether an accreditation or certification framework for cyber security professionals may improve the cyber skill base in Australia. Some directors consider that a professional accreditation framework, particularly for senior or highly technical cyber security professionals, may assist in providing confidence that a senior professional meets certain industry standards and level of education.

However, we recognise that a requirement for professional accreditation can raise barriers and costs for people to enter a particular professional field. Government analysis of this proposal should examine this trade off, including whether accreditation would ultimately limit the number of people that seek to become a cyber security professional, particular in entry level jobs, due to cost or particular educational barriers.

[11] Per Capita and CyberCX, *Upskilling and Expanding the Australian Cyber Security Workforce*, October 2022.

3. Director duties and obligations

2c. Should the obligations of company directors specifically address cyber security risks and consequences?

Strength of existing director duties

The AICD considers that Australia's existing statutory and common law directors' duties provide a comprehensive and clear legal framework that obliges directors to effectively oversee the management of cyber security risk and build cyber security resilience.

The introduction of a specific cyber duty for directors, or mandatory governance standards, would be an unnecessary and burdensome regulatory reform with unintended consequences and limited benefit. In our view, it would also be premature given the lack of clear guidance from Government on what is expected of directors in this area. Despite two major data breaches in Australia in late 2022, Government has not shared with industry, or the public more broadly, the key lessons for directors and senior management resulting from these incidents. To our knowledge, the Cyber Principles have thus far been the most extensive guidance that sets out a cyber governance framework for directors against the backdrop of Australia's cyber and privacy legal and regulatory landscape, and even that document was only released in October 2022.

As discussed below, entities already face a range of legal, regulatory and reputational risks, both in terms of corporate and personal liability, if they fail to give sufficient focus to the oversight of cyber security risk, resilience and preparedness. It would also be a novel approach when compared to similar jurisdictions. The KWM analysis (Attachment B) finds that **there is no comparable overseas jurisdiction that has introduced specific economy wide cyber specific director duties and/or mandatory governance standards**.

A considerable strength of Australia's principles-based directors' duties framework is that it provides sufficient flexibility to ensure directors are proactively overseeing emerging risks (for example, cyber or climate change). The Corporations Act directors' duties that are most relevant to cyber are:

- **Duty to act with care and diligence**: Section 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. As noted above, we are not aware of any credible stakeholder suggesting that a director could not *currently* face liability under section 180 for poor cyber risk oversight. Where ASIC becomes aware of poor board cyber practices, we would encourage them to utilise the full range of enforcement mechanisms available to them, including initiating civil penalty proceedings.

- **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. A recent legal opinion by Bret Walker SC and Gerald Ng commissioned by the AICD confirmed that the duty to act in the best interests of the organisation cannot be isolated from the interests of its stakeholders and directors have considerable latitude to factor stakeholder interests into decision making.[12]

Our view, and that of all legal practitioners that we have engaged with, is that an organisation's cyber security resilience is directly relevant to a director meeting their existing statutory and common law duties. ASIC has issued several statements on cyber preparedness, emphasising the importance of active engagement and oversight by the board. The recent *ASIC v RI Advice* case, although prosecuted under specific Australian Financial Services Licence (**AFSL**) laws, has demonstrated ASIC's willingness to take action against entities that fail to adequately mange cyber risks.[13]

As the Cyber Principles state, while it is not the role of the board to directly manage cyber risk, it is the board that has ultimate accountability for how risks are governed and addressed. This includes being satisfied there are appropriate processes and delegations in place that provide directors with comprehensive oversight of the actions of management. The Cyber Principles make clear that while in some circumstances directors may rely on information or the advice of others, or delegate certain matters to a board committee or senior management, this does not absolve directors of their accountability for decision-making. All directors must have a sufficient understanding of cyber security risks to allow effective oversight of management and risk.

Two recently commenced enforcement actions against the directors of Star Entertainment Group and TerraCom Limited highlight ASIC's increased appetite to pursue directors for alleged breaches of section 180 in relation to the governance of non-financial risks.[14] Our expectation, based on public comments, is that ASIC will also pursue directors in future under section 180 for failing to appropriately govern cyber security risk.

It is important to highlight the liability backdrop against which Australian directors' duties operate in Australia. In 2020, the AICD commissioned law firm Allens to research criminal and civil liability settings on directors in Australia and in comparative jurisdictions (the UK, New Zealand, Canada, Hong Kong and the USA). **Allens concluded that Australia's director liability environment is unique - and in many regards, uniquely burdensome - as compared with other jurisdictions**.[15]

A contributing factor to this uniquely burdensome director liability environment is how a breach of the law by an entity can lead to director liability via the 'stepping stone' doctrine.[16] This form of 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. 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.

Introducing a specific director's duty or mandatory governance standards for cyber security resilience would require the Government to clarify how it would be distinct from the well-established section 180

[12] Bret Walker SC and Gerald NG legal opinion: Directors' "Best Interest" Duty, available here.
[13] ASIC media release, *RI Advice*, available here.
[14] In the case of the directors of Star Entertainment Group, for alleged failures to give sufficient focus to the risk of money laundering and criminal associations. In the case of TerraCom Limited, for alleged failures to take reasonable steps upon receipt of a whistleblower's report or provide sufficient protections to the whistleblower.
[15] Allens research available here.
[16] Ibid.

duty of care and diligence under the Corporations Act. It would also require a fault threshold for a breach to be established and an accompanying model of expected practice. For instance, a possible fault threshold may be a failure to take 'reasonable steps' to develop and maintain cyber resilience. Our view is that what constitutes 'reasonable steps' in cyber security from a governance perspective is exceedingly complex to determine, as it is constantly evolving and will be dependent on the unique circumstances of the entity. As noted above, there is currently very limited guidance from the Government as to the regulatory expectations of directors, and no direct case law.

Accordingly, we consider section 180 of the Corporations Act (duty of care and diligence) is the best suited regulatory mechanism to apply to directors' governance of cyber risk. An advantage of that provision is that it takes into account the circumstances of the company and the position and responsibilities of the relevant director or officer. The standard of care required will vary depending on the type of entity - that could include whether it is proprietary or publicly listed or unlisted, the size and nature of the business, as well as unique risks it may face.

Unnecessary layering of additional liability

The Government already has a number of regulatory frameworks that focus the mind of directors, and the organisations they govern, on the oversight of cyber security risk and data management. The AICD's view is that pursing additional forms of board level liability for cyber security is not only unnecessary but could result in significant unintended consequences.

In the following table we have listed the relevant existing and proposed regulatory obligations relevant to cyber security. Overwhelming feedback from directors is that these regulatory regimes achieve their purpose in focusing their boards and senior management teams on proactively managing cyber security risk. This regulatory dynamic is reinforced for directors by the considerable reputational and financial damage that can come with significant cyber security attacks, as discussed above.

Regime	Relevant to the governance and management of cyber security risk
Corporations Act	• Directors' duties • Australian financial services licence risk management obligations • Continuous disclosure obligations • Misleading and deceptive conduct provisions
Privacy Act	• APP 11 Security of personal information (proposed to be enhanced under the Privacy Act Review) • Notifiable Data Breaches (**NDB**) scheme (proposed to be enhanced under the Privacy Act Review) • Office of the Australian Information Commissioner (**OAIC**) conciliation process • Significant penalties for serious and repeated breaches of the Privacy Act • Low and mid-tier penalty provisions (proposed under the Privacy Act Review) • Class action risk (a direct right of action is proposed under the Privacy Act Review)
SOCI Act	• Create and maintain a critical infrastructure risk management program, including annual board attestation • Enhanced cyber security obligations required for operators of systems of national significance • Register of Critical Infrastructure Assets • Mandatory reporting requirements • Government assistance and intervention powers

Industry specific obligations	• Australian Prudential Regulation Authority (**APRA**) prudential requirements (CPS 234, CPS 230 – proposed) • *My Health Records Act 2012* • ASIC Market Integrity Rules • Australian Energy Sector Cyber Security Framework • *Telecommunications Act 1997*
Australian Consumer Law (**ACL**)	• Collection and use of personal information (Medibank facing class action activity under the ACL associated with data breaches)
Consumer Data Right	• 13 privacy safeguards, contained in the *Competition and Consumer Act 2010* (Cth) and supplemented by the Consumer Data Rules, which is enforced by the OAIC.

Imposing additional liability on directors, in circumstances where the extent of the risk is constantly evolving and complex is, in our view, unreasonable and inappropriate.

An important distinction must also be drawn between the oversight of cyber security risks and work, health and safety (**WHS**) risks that entities face. Unlike the management of WHS risks, even entities with the most rigorous cyber security practices, that take all reasonable steps to protect their systems and data, can fall victim to sophisticated, sometimes state-sponsored, cyber-attacks. Certain entities may face heightened exposure given their critical role in the Australian economy (e.g. critical infrastructure providers), and volatile nature of geo-politics. Unlike with WHS, organised criminals are actively seeking to breach organisations' cyber defences. It is critical that liability settings reflect this reality rather than taking a punitive approach that assumes that more regulation will safeguard organisations from breaches.

The AICD is concerned that creating further liability or additional layers of regulation at the board level would result in preoccupation with compliance and personal liability, at the expense of innovative and dynamic approaches to building cyber resilience.

More generally, we are concerned with the seemingly reactive and piecemeal approach to regulation that seeks to respond to emerging enterprise risks with a focus on imposing new forms of personal liability on the leaders of Australia's businesses. This is a punitive and narrow compliance focused approach to policy making. The AICD's strong preference is for a partnership model that balances risk-focused regulation with industry collaboration and support.

Multiple regulatory enforcement mechanisms and class action risks

In considering additional cyber specific directors' duties, it is critical to note the interaction with proposals recommended in the Privacy Act Review. These include a possible new direct right of action and separately, a statutory tort for invasions of privacy. These mechanisms, if introduced, will enable individual and class action claims against entities where affected individuals suffer loss or damage as a result of an interference with their privacy, including by way of a data breach.

As highlighted in the AICD's submission to the Privacy Act Review Final Report, it is important to have regard to the interaction and cumulative effect of the multiple regulatory and compensatory mechanisms – both existing and proposed.[17] For example, to illustrate the various liability avenues available at both the corporate and individual director level, an entity that suffers a data breach as a result of a cyber attack may face:

[17] AICD submission to the Privacy Act Review Final Report, available here.

- the imposition of penalties by the OAIC for a breach of the Privacy Act;
- if legislated, a direct right of action claim for compensation and a separate statutory tort action brought by affected individuals suffering loss or damage (extending to humiliation and injury to a person's feelings) as a result of the breach;
- if the entity is regulated by APRA, enforcement action for a breach of Prudential Standard CPS 234 Information Security;
- if the entity holds an AFSL, enforcement action by ASIC for a breach of AFSL risk management obligations;
- if the entity is subject to the proposed Financial Accountability Regime, enforcement action alleging a breach of its accountability obligations (including acting with care and diligence and taking reasonable steps to prevent matters arising that would adversely affect the prudential standing or reputation of the entity);
- if the entity is listed, and there is a material impact to the entity's share price, a securities class action on behalf of shareholders alleging the entity breached its continuous disclosure obligations by failing to adequately disclose their privacy risks and vulnerabilities; and
- enforcement action by ASIC against the individual directors and officers of the entity for a breach of section 180 of the Corporations Act, either via the stepping stone approach to liability due to the breach of the Privacy Act, or more directly for failing to take reasonable steps to ensure appropriate policies, procedures and systems were in place to prevent a breach and protect data held by the entity.

For completeness, we accept it is appropriate that an entity face these range of enforcement and compensatory actions provided there has been *significant fault* on the part of an entity and its directors and officers in failing to mitigate the risk of a breach.

Against this backdrop, however, we do not consider there is a convincing policy case for imposing additional personal liability on directors for overseeing cyber risk. It would also run counter to established principles of law against "double punishment". The Australian Law Reform Commission (**ALRC**) has cautioned against legislative and regulatory design that results in multiple civil penalties attaching to the same conduct.[18]

If nonetheless, the Government decides to legislate such a duty, enforcement should be reserved for regulators who would assess cases in the public interest rather than private litigants and plaintiff law firms who may see the high threat cyber environment as ripe for profitable litigation.

Risk Management Program model

The AICD considers that were the Government to conclude that directors' focus and oversight of cyber security needs to be elevated, the Risk Management Program (**RMP**) provisions under the SOCI Act may represent a policy model that could be assessed further.

[18] ALRC, 'Principled Regulation: Federal Civil and Administrative Penalties in Australia (ALRC Report 95), Chapter 11, available here.

While the RMP provisions cover risk management practices broader than just cyber security, they may represent a template for a set of risk management principles sitting outside the SOCI Act that could be applied more broadly.

Under the RMP provisions, entities have flexibility to determine how to address material risks and the relevant impacts taking account of their business size, maturity, income and overall asset criticality. A key mechanism for accountability is that the Board of the entity must annually approve a report on the RMP that is provided to the regulator. This straightforward mechanism ensures that the RMP is considered closely by the Board and whether it is satisfied that the RMP is up to date and reflects the key requirements under the SOCI Act. We also consider the ability of the RMP provisions to account for other equivalent regulatory regimes, such as APRA prudential requirements, is a strength that assists in limiting complexity for entities.

We recognise there would be challenges in utilising this model for a broader population of entities and it may not be appropriate for all elements of the RMP obligations to be extended beyond the SOCI Act. For example, many organisations rely on key third party providers for key digital and information technology services and products. We understand there are already challenges in gaining assurance on the cyber security standards of these key providers and these challenges would only be magnified across a larger population of entities.

We also consider that ultimately were this policy option to be pursued, it should be limited to large businesses only, reflecting the limited resources and capacity of SMEs and NFPs to meet legislated risk management requirements.

The AICD would in-principle support the Government undertaking further analysis of whether an RMP type model may be appropriately adapted for a broader cohort of large businesses.

4. Legislative architecture

2b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

The AICD does not support further amendments to the SOCI Act in the short term. While we in-principle would not oppose an expanded definition of 'critical assets', our strong view is that the Government's priority, via the Cyber and Infrastructure Security Centre, should be raising awareness of the SOCI Act obligations rather than pursuing further amendments at this time.

The SOCI Act is a new legislative framework that underwent significant amendments in late 2021 and early 2022, including substantially expanding the number of entities caught as critical asset owners. The expanded SOCI Act is still in the process of being implemented by critical asset owners, with notably the Risk Management Program rules recently commencing. **We note that the KWM analysis highlighted that Australia currently has some of the strongest cyber specific obligations on directors in respect of critical infrastructure or systems of national significance** when compared to other jurisdictions.

We have received feedback from industry advisors that there are significant gaps and a lack of an understanding of the SOCI obligations amongst entities caught under the recent expansion, for example privately owned businesses in the transport sector.

Ensuring the SOCI Act is understood and being complied with by the regulated population should be the current priority rather than pursuing further legislative change.

We understand that the question of an expanded definition to include 'customer data and systems' is informed by the Government's experience of assisting large organisations' experience with significant cyber incidents and data breaches over the past six months. Based on the very limited publicly available information on these incidents, it is not clear how an expanded definition would have assisted a coordinated Government response or improved outcomes or communications for impacted individuals. It is not apparent how the use of directive powers under the SOCI Act would have limited the damage of the attack, provided additional support or improved impacted customers understanding of the resulting data breaches.

Were the Government to pursue amendments focused on the definition of critical assets, we would strongly recommend that it explain the policy rationale for the change and how it will enable the Government to more effectively assist impacted critical asset owners in a significant incident.

More generally, we encourage the Government to review the effectiveness of the SOCI Act amendments after an appropriate period, for example 3 years. Such a time period will allow an informed assessment of whether the SOCI Act has achieved a strengthening of the resilience of Australia's critical asset owners and systems of national significance.

2d. Should Australia consider a Cyber Security Act, and what should this include?

The AICD in-principle supports a standalone Cyber Security Act (**CSA**) that consolidated and harmonised existing regulatory obligations within one legislative framework. A well-designed, comprehensive and flexible CSA would provide much needed clarity on cyber security regulatory obligations to the benefit of all stakeholders, including regulators and Government agencies.

We would not however support a CSA that was utilised to introduce new obligations on organisations and directors resulting in a layering of regulatory requirements over existing multiple regulatory regimes.

As discussed above, the AICD has consistently received feedback from directors on the existing complexity and overlapping nature of cyber security and data management regulatory obligations in Australia.

Directors report that this complexity is increasing with the recent amendments to the SOCI Act, more prescriptive and onerous APRA prudential requirements and amendments to the Privacy Act. Reporting and notification requirements, data retention obligations, risk management obligations and expectations as well as roles of key regulators are areas raised as requiring streamlining and harmonisation.

The AICD's submission to the Privacy Act Review Final Report strongly supported work to harmonise data retention requirements across the Commonwealth and States as a necessary pre-condition to strengthening individual rights under the Privacy Act.

We have received feedback from both AICD members and industry experts on the current challenges with interpreting, navigating and complying with Commonwealth, State and industry specific data retention laws and law enforcement obligations. As a consequence, organisations will hold personal information for extended periods out of an abundance of caution to ensure they are meeting any applicable obligations.

The AICD's view is that this regulatory complexity is a key contributing factor to entities holding personal information for longer than is necessary, which in turn increases the extent of data loss and potential damage from a significant cyber incident or data breach.

Just as there is a valuable opportunity for the Privacy Act review to address these challenges with data retention laws, we similarly consider that a CSA represents an opportunity to make important progress in streamlining, consolidating and clarifying regulatory requirements in the following areas:

1. A single reporting or notification portal for cyber and data incidents and breaches – discussed in greater detail below in response to question 13a;

2. Additional reporting obligations in respect ransomware and data extortion incidents – discussed in greater detail below in response to 9;

3. Clarification of the roles and responsibilities of regulators and Government agencies in overseeing cyber security and data management requirements, including assistance in the event of a significant cyber security and enforcement responsibility in respect of any breaches. This clarity on roles would cover the recently announced Coordinator for Cyber Security, Australian Signals Directorate/ACSC, Department of Home Affairs, Office of the Australian Information Commissioner and industry specific regulators, such as Australian Communications and Media Authority (**ACMA**) and APRA;

4. Confidentiality and regulator information sharing provisions – discussed in greater detail below in response to questions 7 and 8; and

5. Risk management obligations. As discussed above in response to question 2c, the AICD would in-principle support the Government undertaking further analysis of whether an RMP type model may be appropriate to be applied to a wider set of large businesses.

In addition to the above, we recommend that policy analysis of this proposal should explore the degree to which core components of the SOCI Act, Privacy Act and industry obligations can be incorporated or referenced in a CSA. Again, we consider that the effectiveness of a CSA would be significantly weakened were there to continue to be disparate regimes sitting outside of a CSA – adding to, rather than, streamlining the existing patchwork of cyber-related regulatory regimes.

The ALRC has highlighted its concerns that legislative complexity can create greater challenges for achieving compliance, impose additional costs for both the regulated and the regulator, and risk uncertainty in the meaning of the legislation.[19] In a similar vein, Commissioner Kenneth Hayne noted in the Financial Services Royal Commission Final Report that legislative complexity "*can cause the regulated community to lose sight of what the law is intending to achieve and instead see the law as no more than a series of hurdles to be jumped or compliance boxes to be ticked*".[20]

The AICD recommends that any further policy development work on a CSA be the subject of extensive consultation with industry.

6. Ransomware and data extortion

2f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:

(a) victims of cybercrime; and/or

[19] ALRC, Legislative Framework for Corporations and Financial Services Regulation: Complexity and Legislative Design, October 202, available here.

[20] Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, Interim Report (Volume 1, 2018) 162.

(b) insurers? If so, under what circumstances?

i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

The AICD is not convinced that a strict prohibition on the payment of ransoms and extortion demands by either victims or insurers is appropriate. There are already certain laws in place in Australia that mean doing so could amount to a criminal offence relating to instruments of crime and financing terrorism, depending on the facts.[21]

As a general principle, we consider it is critical that entities are discouraged from paying a ransom or extortion demand. As discussed further below, Government clarifying its position with respect to payment of ransoms would support more informed board decision-making when faced with a demand. This would particularly be the case for SME and NFP entities that may not have the same access to expert advice in these circumstances.

The AICD recognises the considerable complexity involved for entities in responding to a ransomware or similar extortion demand. According to the ACSC, ransomware remains the most destructive cybercrime due to its multifaceted impact.[22] Not only are entities' systems and operations disrupted by the encryption of data, but there are also ongoing costs associated with system reconstruction, lost productivity, lost customers and reputational damage.

In feedback to the AICD over recent years, directors have expressed mixed views on whether a legislative prohibition on ransom payments would assist board decision making when faced with a demand or reduce the prevalence of ransomware across the Australian economy.

On balance, the AICD is concerned that a legislative prohibition would be a blunt instrument. There is a need to preserve a degree of flexibility so that entities, with the support of insurers and expert advisers, may determine the appropriate course of action. Factors commonly weighed can include physical safety, threats to solvency or critical operations, the nature and extent to which data and/or systems have been compromised, the prospects of recovery and privacy and other risks for the individuals affected if data is released or sold on. In considering such issues, directors' duties of care and diligence, and to act in the best interests of the corporations they govern, apply.

Entities in certain sectors, such as critical infrastructure and essential services, may have a greater imperative to pay a ransom in order to keep systems operational and if individuals' health and safety are at risk. Examples often cited include hospitals, utilities, transport, energy and telecommunications.

The AICD is also cautious about proposals for a 'safe harbour' exception to operate alongside a legislative prohibition on ransom payments, enabling entities to pay a ransom in limited and exceptional circumstances. This could lead to unintended consequences by increasing the risk exposure of entities in specific sectors, or incentivising attacks on entities outside of those sectors who may not qualify for the 'safe harbour' but may face potentially existential consequences if they do not pay. In other words, it could drive ransom payment activity underground - at odds with the Government's aim to improve the transparency around the nature and scale of ransomware and extortion in Australia.

Were Australia to legislate a strict prohibition on ransom payments, we would be a global outlier. To date no other jurisdiction has introduced a legislative ban on ransom payments. This is a concern cited by

[21] Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and the Criminal Code Act 1995 (Cth).
[22] ACSC Annual Cyber Threat Report, July 2021 to June 2022, accessible here.

multi-national organisations that have cross-border data flows and as highlighted in the KWM Research, are subject to varying legal and regulatory obligations in respect of data protection and privacy.

It is important that, as a global issue, regulatory measures in respect of ransomware are in alignment with legislators and regulators in other jurisdictions. We discuss further below our views on the role for Government to support industry respond to ransomware and extortion demands.

Class action risks associated with ransom payments

As noted above, it is critical to consider the impact a prohibition on ransom payments could have on key proposals, such as the direct right of action and statutory tort for invasions of privacy, being contemplated separately under the Privacy Act Review.

In practice, these reforms, if implemented, would mean that where entities are the victims of a data breach as a result of a ransomware attack and do not pay a ransom to secure the return of that data, the entity may face claims for compensation by affected individuals who suffer loss or damage as a result of that data being released or sold on. This would be a perverse policy outcome and in fact, may operate to incentivise the payment of ransoms should an entity consider it would incur less costs in doing so, compared with a data breach class action.

In our view, regardless of whether Government is minded to legislate a prohibition on ransom and extortion payments, entities which do *not* pay a ransom should not then be exposed to actions under the Privacy Act for loss of data and interferences with privacy – either regulatory or compensatory – unless there was significant fault by the entity that led to the data breach.[23] A similar approach should be taken to any other cyber related proceeding – that is, significant fault must be demonstrated to ground a claim.

The AICD strongly encourages cross-Government coordination on this issue to ensure any policy measures taken do not produce misaligned cyber and privacy regulatory outcomes.

2g. Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?

The AICD supports the Government clarifying its position with respect to payment or non-payment of ransoms and the circumstances in which this may constitute a breach of Australian law.

While we do not support a strict prohibition on the payment of ransoms for the reasons discussed above, clarification from Government on its position and the legality of ransom payments would support more informed board decision making when face with a demand. We also consider this would benefit SMEs and NFPs, in particular, who may not have access to expert advice from insurers or expert advisers when faced with a demand.

The AICD further strongly encourages enhanced guidance and support from Government in respect of ransomware as a specific form of cybercrime. Our consultation with directors suggests there is significant demand for practical guidance, training, and Government advice, particularly for SMEs and NFPs. Focus should be given to education and awareness raising campaigns, as well as Government's role in simplifying reporting obligations to aid transparency around the prevalence of attacks in Australia as discussed further below.

[23] For further detail, see AICD submission to the Privacy Act Review Final Report, available here.

7. Reporting obligations and information sharing

9. Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?

The AICD in-principle supports all large businesses being required to notify ransomware and data extortion incidents.

We note the findings of the ACSC that cybercrime, particularly ransomware, is likely to be underreported in Australia.[24] This underreporting limits the visibility that the Government has of the extent of the data extortion problem and impedes intelligence on where threats and attacks are originating from and where ransomware payments are being directed, including to state based actors or particular criminal groups.

All organisations should be voluntarily encouraged and supported to report ransomware incidents to the ACSC. However, mandatory ransomware reporting requirements should be limited to large businesses that have the resources to be aware of the obligation and make the notification consistent with the intent of the requirement. A threshold would represent a balanced and risk-based approach to cyber policy making, reflecting that large businesses frequently hold, in aggregate, the most sensitive individual data at risk from a ransomware attack and are the target of attacks that seek the highest payments. They are also the entities that will be in the position to provide access and further information to the ACSC, or other agencies, on the incident.

As a starting point we consider that a $100 million annual turnover would be an appropriate threshold to apply a reporting requirement. This threshold would align with the current reporting requirements under the *Modern Slavery Act 2018* and would generally capture entities that are large enough to be aware of the reporting obligation and have the resources to make the necessary report.

We would be concerned otherwise that applying a new mandatory reporting requirement to all businesses, or a low threshold (e.g. $10 million annual turnover), would capture entities that do not have the resources to appropriately meet additional reporting requirements, or the impact to justify the cost of regulation. This is likely to be the case with SMEs and NFPs where there would be challenges in providing the necessary support and education on new reporting requirements. Further, a threshold that is set too low may result in contradictory enforcement outcomes where an SME is penalised for inadvertently failing to meet a reporting requirement, in addition to experiencing the costs and disruption of a ransomware incident.

We recognise that exempting SMEs from a ransomware reporting requirement may impact the depth or scope of information collected. Nonetheless, we are not satisfied that a mandatory obligation applied to SMEs would result in sufficient compliance in any event to materially improve the visibility or understanding of ransomware activity in Australia for this segment of businesses. Instead, we consider the Government should focus on incentivising voluntary reporting by SMEs, including through assistance and guidance for those entities responding or recovering from a ransomware demand.

The AICD stands ready to support consultation on new ransomware reporting requirements, including facilitating engagement with members.

[24] ACSC Annual Cyber Threat Report, November 2022.

13a. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?

The AICD strongly supports the establishment of a single reporting portal for all cyber and data breach incidents. For an entity that is responding to a significant cyber incident and resulting data breach, it can be resource intensive, complex and unnecessary to meet separate notification obligations for distinct Commonwealth regulators.

We consider that the existing SOCI and voluntary cyber incident notification processes overseen by the ACSC would be a starting point for the establishment of a single portal.

We note that the Productivity Commission expressly recommended a single portal model (Recommendation 4.5) under its Productivity Inquiry, finding:

> *A business may face multiple reporting requirements for a single cyber security incident, depending on its operations and the nature of the breach. This can place unnecessary burdens on businesses that are focused on recovering from the cyber incident. More coordination between government agencies and streamlining of reporting requirements (such as via a single online interface) would assist in reducing reporting burdens on businesses.*

While the AICD appreciates that different reporting and notification regimes are established for different purposes by distinct regulators or legislative regimes, this should not be an insurmountable barrier to the use of a single portal. A dynamic and intuitive portal would importantly lessen the burden on an entity in meeting various reporting obligations, particularly where harmonisation of the specific reporting framework is not possible. The portal could have features where a reporting entity provides permission and direction for the data to be shared with applicable regulators.

For instance, a financial services entity notifies a data breach via the portal in respect of SOCI Act and the Notifiable Data Breaches scheme and provides permission for this data to also be shared with APRA. The portal could have design features that prompt additional information where necessary depending on specific industry obligations.

A single portal would also assist in coordination of the Government response to a particular cyber incident, including clarifying responsibilities of which regulator or agency will take the lead in assisting the entity.

We have received feedback from directors that have experienced significant cyber incidents at larger businesses, that the Government response can be disjointed and uncoordinated, with the same information requested by different agencies and regulators.

We understand that the National Coordination Mechanism has assisted a coordinated response in recent significant cyber security incidents. However, this is not a sustainable model for all cyber security incidents. A well-designed portal could help in clarifying responsibilities and incorporate mechanisms to allow for further requests for information and provide assistance or resources for impacted entities, such as directing the entity to ACSC guidance.

7. What can government do to improve information sharing with industry on cyber threats?

The AICD recognises the extensive work the ACSC currently undertakes in sharing intelligence with industry, publishing alerts and developing guidance on cyber security threats.

Feedback from directors is that for participating organisations the ACSC Partnership Program, particularly as an ACSC Network Partner, is seen as an effective way for the ACSC to share latest threat intelligence and highlight alerts with larger businesses. However, more could be done to lift market awareness of the availability of this valuable program.

The of a broad-based confidentiality regime would also support an elevated level of trust and information sharing between the ACSC, other agencies and industry.

More broadly, we encourage the ACSC to share with industry examples or case studies of best practice in building cyber resilience and responding to significant cyber security incidents. While the sharing of threat intelligence is critical, industry is also seeking an understanding of what 'good looks like'. These examples or case studies could be anonymised but importantly convey in a comprehensive manner how a particular entity has sought to build its resilience or responded/recovered from a cyber security attack.

The AICD considers that the focus of enhancing threat intelligence and broader cyber security guidance should be on SMEs and NFPs, including directors of these organisations. While the ACSC website has extensive resources, which are regularly updated, we perceive a low awareness of this guidance amongst SMEs and NFPs. Raising awareness could be done in conjunction with other regulators, state/territory governments and/or relevant industry bodies.

For instance, for many SMEs and their advisors, the Australian Taxation Office (**ATO**) is a regulator they regularly interact with and the ATO may have tools that can call attention to particular ACSC alerts. As discussed above, we consider there is merit in a public information campaign targeted at SMEs and individuals to raise awareness of the ACSC and cyber security threats and safety.

The AICD encourages the Government to explore creative and dynamic methods of raising awareness of the cyber threat landscape and practical steps that organisations of all sizes can take to enhance their resilience. The AICD stands ready to assist those efforts.

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?

The AICD strongly supports explicit confidentiality obligations on the ASD (encompassing the ACSC) in respect of information provided to it by organisations sharing cyber threat intelligence and notifying, and seeking assistance, in respect of a significant cyber incident.

We consider that a confidentiality regime would promote trust and collaboration between Government and industry responding to significant cyber security incidents and incentivising timely and complete reporting. It would also importantly signal that Government is committed to embedding a partnership-based approach to addressing cyber security threats and building cyber security resilience across the economy.

Our view is that a confidentiality regime should not just be limited to a cyber security incident but be sufficiently broad to encompass both information sharing initiated by an entity (including under mandatory notification/reporting requirements), proactive information gathering by the ACSC and existing threat and intelligence sharing mechanisms (e.g. ACSC Partnership Program).

Taking a broader approach to the design of this regime would address scenarios where there can often be opaque and incomplete information on cyber threats and incidents shared across the eco-system. In many cases, pertinent information or intelligence may only be held by some participants in a supply chain (e.g. key service provider). For example, a cloud service provider may hold relevant information on a customer that has experienced data breach. The confidentiality regime should ensure that this provider has confidence that it can share information with the ACSC without fear that it may be utilised for other purposes, including investigation and enforcement activity.

A significant cyber incident can take months to resolve or be closed and a confidentiality regime should be sufficiently flexible to reflect the imprecise nature of when an incident starts and concludes.

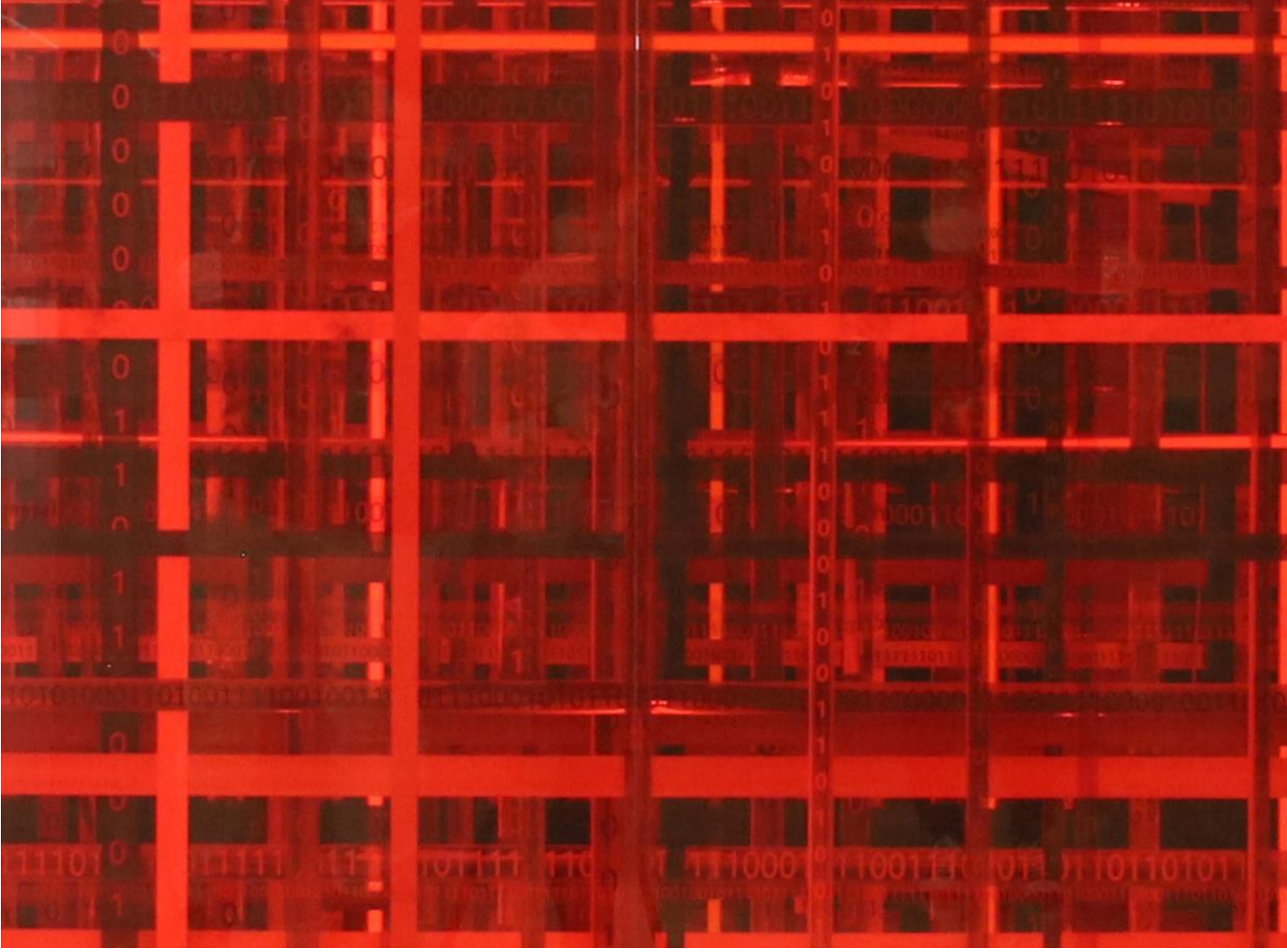
Our understanding is that the ACSC is the lead arm of the Government that assists entities in responding to significant cyber incidents. However, any confidentiality regime may need to encompass other regulators and agencies to provide sufficient coverage and confidence that information freely shared will not be distributed or utilised in a way inconsistent with the purposes it was provided for. For instance, our expectation is that the Cyber and Infrastructure Security Centre and the proposed National Coordinator for Cyber Security would have a role in responding to incidents impacting critical asset owners. Separately, industry-based regulators, such as ACMA and APRA, would likely have roles in incidents impacting their regulated entities.

The AICD considers a well-defined confidentiality regime applying to relevant Commonwealth agencies is consistent with clarifying the roles and responsibilities of these agencies. The confidentiality regime itself would then be underpinned by a memorandum of understanding (**MoU**) between the relevant bodies on how and when information would be shared.

Our view is that the secrecy and confidentiality provisions that apply to APRA under the *Australian Prudential Regulation Authority Act 1998* (Cth) may be a model that can be utilised by ASD and other regulators in respect of collecting information from entities about a cyber security incident or broader threat intelligence.

We encourage comprehensive industry consultation on this proposal reflecting the legal and drafting complexity of confidentiality and secrecy provisions.

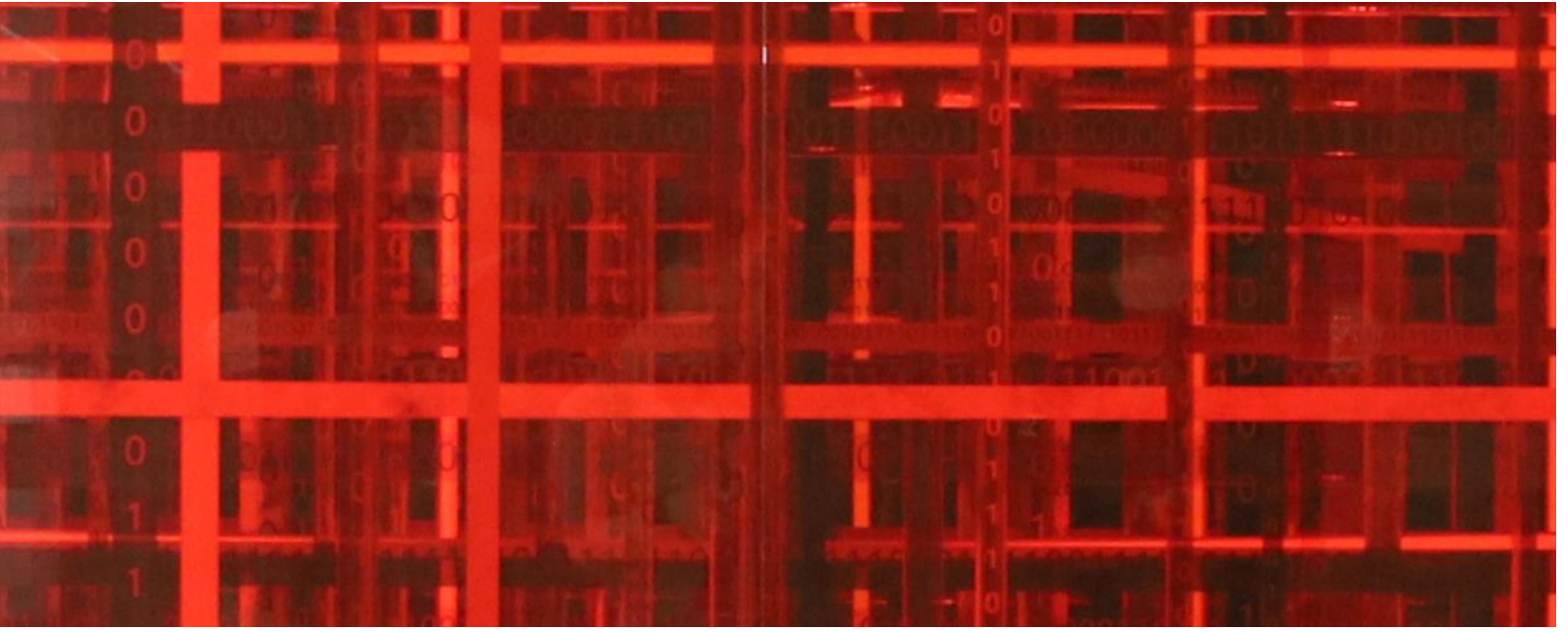
Attachment B – King & Wood Mallesons research



REPORT FOR THE AUSTRALIAN INSTITUTE OF COMPANY DIRECTORS

INTERNATIONAL COMPARISON: CYBER SECURITY OBLIGATIONS

KING&WOOD MALLESONS



ATTRIBUTIONS

DAVIES

Davies Ward Phillips & Vineberg LLP

Canada

fieldfisher

Fieldfisher

UK & EU

DISCLAIMER

This report does not constitute legal advice and you should obtain legal advice before relying on any part of it. The content must not be reproduced without permission from King & Wood Mallesons.

King & Wood Mallesons refers to the network of firms which are members of the King & Wood Mallesons network.
Legal services are provided independently by each of the separate member firms. No member firm nor any of its partners or members acts as agent for any other member firm or any of its partners or members. No individual partner or member in any member firm has authority to bind any other member firm. See **kwm.com** for more information.

AICD: INTERNATIONAL COMPARISON OF CYBER SECURITY OBLIGATIONS

Table of Contents

KING&WOOD MALLESONS

1. Executive Summary

Australia continues to face an increasingly challenging cyber security environment. Threats and data breaches continue to increase almost daily, without an end in sight. The Australian Government has therefore made it a priority to focus on uplifting Australia's cyber security and has a vision to make Australia the world's most cyber secure country by 2030.

To bring this vision to life, the Government is developing its 2023-2030 Australian Cyber Security Strategy. Its Expert Advisory Board recently published the 2023-2030 Australian Cyber Security Strategy Discussion Paper, which seeks feedback on core cyber security policy areas and discusses potential cyber security reform measures. Importantly, the Strategy Paper canvasses the potential to introduce new and enhanced obligations for Australian companies to specifically address cyber security risks and consequences.

In this context, the Australian Institute of Company Directors has asked King & Wood Mallesons to undertake a comparative analysis of existing and proposed cyber security obligations in Australia against those in the United States[1], Canada[2], the European Union and the United Kingdom.

The purpose of this comparison is to contextualise Australia's regulatory landscape and the Australian Government's approach to cyber security and to identify key cyber security regulatory themes that are trending across the Comparator Jurisdictions. Our comparison does this around the following themes:

(a) board accountability and governance;

(b) sector-specific cyber security obligations;

(c) future directions in regulation; and

(d) increasing international coordination response to cyber incidents.

Some key findings that emerge from these themes are that:

(a) there are no general duties imposed on directors in relation to cyber security in any Comparator Jurisdiction;

(b) there is a trend to imposing cyber security responsibilities on directors under industry-specific regulatory frameworks; and

(c) Australia currently[3] imposes stronger cyber specific obligations on directors in respect of critical infrastructure or systems of national significance when compared against other Comparator Jurisdictions.

Overall, the international cyber regulatory landscape is clearly in a state of flux. However, in general, each of the other Comparator Jurisdictions share common cyber policy objectives to Australia. Each jurisdiction is implementing regulatory reforms to make them more cyber secure and cyber resilient, often in a way that is increasingly consistent. This is to be expected, given the global nature of cyber security risks and the natural convergence of policy outcomes and mechanisms to address them.

2. Scope of Review

The comparison focuses on cyber security obligations in Australia and each other Comparator Jurisdiction, having particular regard to directors' duties and governance, as at 31 March 2023. In particular, the comparison covers the following areas:

(a) current economy wide cyber security obligations;

(b) specific cyber security obligations that apply to critical assets or systems of national significance;

(c) prominent sector or industry specific cyber security obligations;

(d) reporting and notification obligations attaching to cyber security incidents;

(e) listed company disclosure obligations relating to cyber security incidents;

[1] At a Federal level, noting that States may also have specific cyber security legislation and regulations.

[2] At a Federal level, noting that Provinces and Territories may also have specific cyber security legislation and regulations.

[3] Although these obligations will be comparable to those imposed by the EU under NIS 2 when that comes into effect in October 2024.

(f) class action settings;

(g) presence of direct rights of action or statutory tort arising out of a cyber security or data breach;

(h) identity of key cyber security regulator(s);

(i) level of guidance and support provided to industry by the cyber security regulator;

(j) mechanisms or frameworks to facilitate the sharing of intelligence or support in the event of a significant cyber security incident; and

(k) pending or new developments in cyber security regulation.

It does not address:

(l) criminal law regimes aimed to punish or deter those who seek unauthorised access to computer systems or otherwise commit cyber-crimes[4]; or

(m) merger control regimes directed at security issues.[5]

3. Acknowledgements and contributors

We would like to acknowledge the contribution of the firms who have collaborated with us to produce this comparative survey. These are:

- James Walsh and James Seadon, **Fieldfisher LLP**, London
- Corey Omer, **Davies Ward Phillips and Vineberg LLP**, Montreal
- Vincent Filardo, Jr. & Aaron Wolfson, **King & Wood Mallesons**, New York

[4] For example, the Computer Misuse Act 1990 (UK).

[5] For example, the National Security and Investment Act 2021 (UK).

4. Key themes

4.1 Overview

This section outlines some general themes that emerge from the comparison and our reflections on them. They include our observations on:

- governance and board accountability;
- trends towards stronger sector specific regulation, particularly in relation to critical infrastructure;
- intelligence sharing mechanisms and frameworks;
- increasing internal coordination in response to cyber security incidents; and
- future directions in cyber security regulation.

4.2 Governance and board accountability

(a) There are no general duties imposed on Directors in relation to cyber security

As a general proposition, we find that none of the Comparator Jurisdictions have imposed a general duty on directors to ensure the cyber security of their organisations. In each of the Comparator Jurisdictions, directors have general duties of care, skill and diligence to their organisations. In Australia, these general duties are set out in section 180 of the *Corporations Act 2001 (Cth)*. As a result of these duties, directors should be capable of satisfying themselves that cyber risks are adequately addressed and that organisations are cyber resilient. In the event of a data breach, a director may face claims for breach of these duties, including by regulators (such as ASIC's 'stepping stones' approach under which directors may be pursued for an alleged breach of their statutory duty of care where their acts or omissions have exposed the company to a breach of law or through a derivative action[6].

In this regard, guidance to directors such as the AICD's Cyber Security Governance Principles[7], is helpful to assist directors to understand what is required of them to discharge their duties. Moreover, these principles could also be seen as setting a benchmark by reference to which any claim that a director has failed to exercise their duties of care, skill and diligence is judged.

(b) There is a trend to imposing cyber security responsibilities on directors under industry specific legislative frameworks

In each Comparator Jurisdiction, we see a trend of increasing governance implications and accountability for boards and management in particular industry sectors. For example, in Australia:

- under CPS 234, the board of an APRA-regulated entity is ultimately responsible for ensuring that the entity maintains its information security. The entity has a specific obligation under CPS 234 to clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals; and
- under recent changes made to the *Security of Critical Infrastructure Act 2018 (Cth)*, the board of a responsible entity for a critical infrastructure asset which is required to have a risk management program, will need to satisfy itself as to the adequacy of that program. This is because the board has to approve an annual report to the Department of Home Affairs that among other things, states whether the risk management program was up to date and provides details of how the program was effective during the year.

In the United Kingdom, the PRA has issued *Supervisory Statement SS1/21* that sets out the PRA's expectations for boards of companies in the financial sector in relation to the operational resilience of firms' important business services. It requires boards to collectively possess adequate knowledge, skills and experience to provide constructive challenge to senior management and inform decisions that have consequences for operational resilience.

In the EU, under the *Directive on measures for a high common level of cyber security across the Union (Directive (EU) 2022/2555)* also known as NIS 2, member states must ensure that the management bodies (i.e. boards and directors) of regulated entities approve and oversee the implementation of cyber security risk management measures. This means that management bodies are expected to have the knowledge and skills to comprehend and assess cyber security risks and management practices and their impact on the entity's services and are expected to undertake regular training in this space. Failing to maintain adequate risk oversight may

[6] In the US, although a derivative action is brought by shareholders, it is considered as brought directly by the company.

[7] https://www.aicd.com.au/risk-management/framework/cyber-security/cyber-security-governance-principles.html

expose companies, officers and directors to liability, depending on how NIS 2 is implemented into local laws of EU Member States. This does not seem to have been proposed to apply in the United Kingdom under the package of reforms to *The Network and Information Systems Regulations 2018 (UK)*.

(c) There is increasing scope for actions to be brought directly against directors

In the US, there is a strong precedent of class actions being brought against boards and officers in relation to cyber security. While there are no explicit legislative requirements for directors under cyber security legislation in the US, nor a statutory tort arising out of a cyber security or data breach, actions have been brought on the basis that the board has failed to exercise appropriate oversight of a company's cyber security. For example, following two major data breaches, shareholders of Yahoo! Brought a class action against individual board members and officers, alleging that they had breached fiduciary duties (including duties of care and loyalty) by failing to:

(a) properly disclose the security incidents;

(b) ensure that proper security measures were in place; and

(c) investigate the relevant incident.

The insurance carriers agreed to pay US $29 million to settle the dispute. Actions have also been brought on other grounds, including breaches of express or implied contracts, negligence, other common law torts, or breaches of consumer protection legislation.

There is far less precedent in Australia for direct actions against directors in relation to cyber security. While ASIC successfully took action against a financial services licensee for breaching section 912A of the Corporations Act for failing to ensure adequate cyber security measures were in place,[8] it did not take direct action against the directors of that licensee under their 'stepping stones' approach. It is yet to be seen if the environment will change with the recent proposals in the Attorney-General's Privacy Act Review Report[9] to introduce a direct right of action to enable individuals to apply to the courts for relief in relation to privacy breaches, as well as the introduction of a statutory tort for serious invasions of privacy.

Similarly, in Canada, a new private right of action has been proposed so that affected individuals may seek damages from organisations that have breached privacy legislation. It is also possible that these proposals could result in increased levels of litigation on privacy matters, including through representative groups.

In the EU and UK, there is no explicit cause of action against company directors under the *General Data Protection Regulation (Regulation (EU) 2016/679)* or *Regulation (EU) 2016/679 of the European Parliament and of the Council 2016 (UK)*. However, data subjects may be able to claim compensation from directors in certain circumstances, given that 'natural persons' can be liable for breaches of the GDPR or UK GDPR. More broadly, as data subjects have a direct right of action in the EU, there is clear scope for class actions related to cyber security and data breaches. In the UK, directors can be liable for data protection offences committed with their consent or connivance.

4.3 Stronger sector-specific cyber security obligations to address supply chain and national security risks

Critical infrastructure is a dominating focus of cyber regulatory reforms across all Comparator Jurisdictions. In general, stronger sector-specific cyber security obligations are being introduced to address supply chain and national security risks posed by cyber threats. Additional regulations may also be imposed in important sectors beyond critical infrastructure.

Protection of critical infrastructure

Australia

In Australia, the ongoing reforms to the SOCI Act are central to Australia's national strategy to strengthen cyber security and protect Australian businesses against cyber threats. The SOCI Act applies to 11 critical infrastructure sectors, including communications, data storage or processing, defence, energy, financial services and markets, food and grocery, health care and medical, higher education and research, space technology, transport and water and sewerage.

At present, the SOCI Act requires responsible entities for critical infrastructure assets to:

[8] Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496

[9] https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

(a) provide ownership and operational information relating to critical information assets for inclusion in the Register of Critical Infrastructure Assets;

(b) notify critical and other cyber security incidents to the ACSC online cyber incident reporting portal within 12 to 72 hours, depending on criticality;

(c) comply with Government assistance measures in relation to cyber security incidents, which can include provision of information, compliance with directions, and in some circumstances, allowing Government to undertake certain actions;

(d) if the assets are Systems of National Significance, comply with enhanced cyber security obligations, which can include undertaking statutory incident response planning, undertaking cyber security exercises or vulnerability assessments and providing the ASD with system information; and

(e) most recently, adopt and maintain a critical infrastructure risk management program. The CIRMP Rules set out specific requirements that a CIRMP for a critical infrastructure entity must comply with. These are broken out by subject matter and encompass key hazard vectors. One of the key hazard vectors that the CIRMP must address are cyber and information security hazards. These cover hazards involving improper access or misuse of information or computer systems, or use of a computer system to obtain unauthorised control of or access to the critical infrastructure asset that might impair its functioning. This will include cyber risks to digital systems, computers, datasets, and networks that underpin critical infrastructure systems and includes improper access, misuse, or unauthorised control.

While the SOCI Act does not specifically require a board to approve the CIRMP itself, board approval of the CIRMP should be obtained as part of an entity's normal governance arrangements. This is because the board has to approve an annual report to the Department of Home Affairs relating to the CIRMP and its effectiveness during the year, which will necessarily require the board to satisfy itself as to the adequacy of the CIRMP.

US

Federal regulation in the US is trending in a broadly similar direction in relation to the reporting and notification of incidents in critical industries. The recently passed *Cyber Incident Reporting for Critical Infrastructure Act of 2022* requires the Cyber security and Infrastructure Security Agency, the US federal agency responsible for protecting critical infrastructure, to develop and implement cyber incident reporting regulations. Specifically, the CIRCIA requires covered entities to report certain cyber incidents and ransomware payments to the CISA (e.g. requiring covered entities to report cyber incidents to CISA within 72 hours, as well as an obligation to report a ransomware payment within 24 hours of payment). However, unlike the SOCI Act, which extends to government assistance, risk assessment and planning, the scope of CIRCIA is limited to incident reporting. Accordingly, while it imposes reporting requirements that are similar to those under the SOCI Act, its ambit is comparably limited.

Further, at this stage, the scope of covered entities and covered cyber security incidents have not yet been defined (CIRCIA only requires the Final Rule establishing such definitions to be published no later than September 2025). As such, it is still unclear whether the scope of regulated entities will be comparable to that under the SOCI Act.

Canada

Canada's security of critical infrastructure regime is in the nascent stages. Currently, there is no cyber security legislation that applies specifically to Canada's critical infrastructure. However, in June 2022, the Canadian government introduced *Bill C-26, An Act Respecting Cyber Security*, which, if passed, would enact the *Critical Cyber Systems Protection Act*. The CCSPA would require operators of 'critical cyber systems' to comply with requirements to create, implement and maintain a cyber security program, mitigate supply-chain and third-party risks and report cyber security incidents to the regulator. The scope of covered entities regulated by the CCSPA is narrower than under the SOCI Act, but includes entities such as banks, telecommunications services, pipeline, power line and nuclear energy systems, transportation systems, and clearing and settlement systems.

EU

By comparison, the EU has an advanced and comprehensive framework regulating cyber security of critical infrastructure under:

(a) currently, the Network and Information Security Directive (Directive (EU) 2016/1148), also known as NIS; and

(b) from 18 October 2024, the Directive on measures for a high common level of cyber security across the Union (Directive (EU) 2022/2555), also known as NIS 2.[10]

Broadly, NIS 2 bolsters a company's existing obligations under NIS. NIS 2:

(a) imposes more stringent cyber security incident reporting obligations, including introducing tighter notification timeframes;

(b) requires a company to effect policies and protocols in relation to risk management, information system security, incident handling, business continuity, encryption and cryptography, testing and auditing, vulnerability disclosure, cyber security training and ICT supply chain security;

(c) expands the scope of regulated industries and thereby captures new entities. Notably, it applies the legislation to additional categories of digital infrastructure that were previously not regulated, such as data centre service providers and content delivery network providers;

(d) introduces enhanced sanctions for breach of cyber security risk management and reporting obligations; and

(e) imposes responsibility directly on management to ensure an entity's compliance.

UK

Similar to the EU's NIS, critical infrastructure in the UK is regulated under the UK NIS. The UK NIS imposes obligations on entities providing essential services into various energy, transport, health, water and digital infrastructure sectors ('operators of essential services'). Like the EU NIS, the UK NIS requires OESs to take appropriate and proportionate measures to detect and manage security risks and notify relevant authorities about incidents that have a significant impact on the continuity of the essential services. According to the UK Government, the UK NIS will also be updated to reflect the bolstered obligations under NIS 2, including to:

(a) broaden the scope of the UK NIS to include managed service providers, to keep digital supply chains secure;

(b) improve cyber incident reporting to relevant regulators; and

(c) enable the Information Commissioner to take a more risk-based approach to regulating digital services.

However, it appears that there is currently no proposal to extend liability to boards and directors in relation to cyber security under UK NIS.

Other sector specific regulation

Beyond critical infrastructure, certain significant sectors, particularly financial services and telecommunications, are also subject to sector-specific cyber security obligations.

Financial services

Broadly, there are regulations or legislation in each jurisdiction that impose information security or cyber security requirements on financial entities. In Australia, APRA**'s** Prudential Standard CPS 234 requires regulated entities to:

(a) maintain clear definitions about the information security-related roles and responsibilities of the board and management;

(b) maintain an appropriate information security capability;

(c) implement controls to protect its information assets; and

(d) notify APRA of material information security incidents.

Similar requirements exist:

(a) in the US under the *Gramm-Leach-Bliley Act*, as well as under a rule newly proposed by the Securities and Exchange Commission to impose a more fulsome set of cyber security obligations on US securities market entities;

(b) in Canada under the Canadian *Bank Act 1991* and guidance issued by the OSFI; and

(c) in the EU under the *Digital Operational Resilience Act* and related amending directives.

[10] NIS will be repealed on 17 October 2024. NIS 2 entered into force on 16 January 2023, and member states have until 17 October 2024 to adopt its requirements.

In the UK, the framework comprises standards published by the *Bank of England Prudential Authority in Supervisory Statement SS1/21* and guidance issued by the Financial Conduct Authority, rather than in primary legislation.

In the EU and UK, there are also additional cyber security requirements for payment service providers under *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market* and the *Payment Services Regulations 2017* respectively. These include obligations to notify payment service users where incidents may have an impact on their financial interests and to implement strong customer authentication in accordance with regulatory technical standards.

Telecommunications

In Australia, carriers and carriage service providers in the telecommunications sector have cyber incident notification and reporting obligations under the *Telecommunications (Carriage Service Provider—Security Information) Determination 2022*.

Similar requirements apply in the EU and UK to providers of public electronic communications networks and services. In the UK, the *Telecommunications (Security) Act 2021* requires providers of public electronic communications networks and services to take reasonable steps to bring a security compromise to the attention of persons who use the network or service. Additionally, the *Telecommunications Infrastructure Act 2022* will extend these notification and reporting obligations to UK manufacturers, importers and distributors of smart products.

In Canada, although no specific cyber notification and reporting obligations are imposed on telecommunications service providers, they are required to protect the privacy of their users. This position may change in the near future. Under proposed amendments to the *Telecommunications Act 1993,* the federal government may have the power to impose obligations on telecommunications service providers to secure Canadian telecommunications systems.

In the US, there is no federal legislation specifically regulating cyber security of communication services and networks at this stage. However, cyber security communication services and networks fall under the gambit of FTC and SEC regulations. Further, federal legislation remains open for CISA to include providers of communications services and networks within the scope of entities regulated by CIRCIA. In effect, this would effectively extend the relevant reporting obligations to US companies in the telecommunications sector.

Other sectors

Beyond the financial and telecommunications sectors, there is a range of regulation covering other sectors in the Comparator Jurisdictions. In the US, the Transport Security Administration has issued cyber security directives that will apply to owners and operators of railroad carriers, airports and aircrafts. Health is also often a regulated sector, with federal legislation in the US and provincial legislation in Canada imposing requirements on relevant operators to implement reasonable security policies and procedures. Separately, in the EU, there is proposed legislation that will require operators of artificial intelligence systems used for 'high risk' purposes to be subject to a number of cyber security requirements.

4.4 Stronger cyber intelligence sharing mechanisms and frameworks

In all jurisdictions, there are a range of mechanisms and frameworks to facilitate intelligence sharing and cyber support in relation to cyber security threats and incidents. These mechanisms are largely voluntary. As cyber risks continue to grow and affect both governments and companies, there is a focus on increasing the speed and scale of cyber intelligence sharing and cyber threat blocking. As a result, stronger multidirectional information sharing mechanisms are expected across jurisdictions.

Australia

At present, there are a number of Australian agencies that can provide information and support to companies in relation to a cyber threat or cyber incident. In particular, the ACSC leads the Australian Government's cyber security efforts. Its functions include:

(a) providing cyber security advice and assistance to individuals, businesses and critical infrastructure operators in the event of a cyber security incident;

(b) working with business, government and academic partners and experts in Australia and overseas to investigate and develop solutions to cyber security threats;

(c) operating a national footprint of Joint Cyber Security Centres where it collaborates with business, government and academic partners on current cyber security issues; and

(d) working with law enforcement authorities to fight cybercrime.

AusCERT, which operates under the Joint Cyber Security Centres as part of the ACSC, is also specifically charged to facilitate cyber security threat information sharing and monitoring.

There is no legal obligation to report cyber incidents to the ACSC (except for responsible entities for critical infrastructure assets under the SOCI Act). There is also no requirement to notify the Australian Federal Police, or other Australian law enforcement body, of a cyber incident even though it can be useful to do so.

US

The US Government has identified robust cyber intelligence sharing and victim notification mechanisms as a strategic priority. However, at present, there is limited coordinated cyber intelligence sharing for entities outside critical sectors.

For entities in critical sectors, CISA can help companies to prepare for, respond to, and mitigate cyber threats and incidents. These companies are encouraged to share information about cyber security threats, incidents, vulnerabilities and defensive measures through CISA's Automated Indicator Sharing (**AIS**) tools. These AIS tools enable the real time exchange of cyber threat indicators and defensive measures. Importantly, companies that use the AIS tools are offered anonymity, as well as certain liability and privacy protections to encourage information sharing. However, use of the tools is not mandatory.

Canada

Canadian companies have access to a range of voluntary cyber intelligence sharing frameworks. The Canadian Centre for Cyber Security issues alerts and advice on potential, imminent or actual cyber threats, vulnerabilities or incidents relevant to Canada and Canadians. Beyond the CCS, there is a voluntary platform, the Canadian Cyber Threat Exchange, for private and public organisations to share information and intelligence on cyber attacks. There are also a number of small industry-specific information sharing and analysis centres, which facilitate intelligence sharing among certain members.

EU

In the EU, the mechanisms to facilitate information sharing are more robust. Under NIS, EU member states are required to designate a national single point of contact and create a co-operation network between the contact and the European Union Agency for Cyber security to liaise on NIS risks and incidents. NIS 2 further builds on this by creating a European vulnerability database to allow organisations to voluntarily disclose known cyber vulnerabilities to the network.

NIS 2 also establishes the Cyber Crisis Liaison Organisation Network, which will act as a co-operative network for the national authorities in charge of managing cyber crises in each member state. It is anticipated that EU-CyCLONe will allow such authorities to collaborate and develop timely information sharing and situational awareness.

UK

The UK has strong cyber intelligence sharing mechanisms.

Similar to the EU's NIS, the UK NIS designates the Government Communications Headquarters as the single point of contact. Within the GCHQ, the National Cyber Security Centre specifically provides support to companies during cyber incidents. This provides a single point of contact for organisations, government and the general public. The NCSC:

(a) provides practical guidance on cyber security; and

(b) responds to cyber security incidents to mitigate harms.

The NCSC also has a special division focused on supporting the UK's critical national infrastructure.

Importantly, the Cyber Security Information Sharing Partnership additionally provides registered UK private sector organisations and government departments with a secure and confidential platform to share cyber threat information in real time. This platform enables fast, scaled and multidirectional information sharing. At present, sharing remains voluntary. Beyond these economy-wide frameworks, other UK regulators also provide mechanisms for sharing information about cyber risks within the segments of the market that they regulate.

4.5 Increasing international coordination in response to cyber incidents

Effective international coordination has been recognised as key to addressing and responding to cyber incidents. Accordingly, there has been an increasing effort to scale the emerging model of collaboration by national cyber security stakeholders to cooperate with the international community. For example:

(a) **CRI**: The US has convened the Counter-Ransomware Initiative, an initiative to enhance international cooperation to combat the group of ransomware, build cross-border resilience and collectively disrupt

and defend against malicious actors. The CRI has more than thirty participants, including Australia and the Comparator Jurisdictions, and aims to drive synchronisation of policy and diplomatic efforts between taskforce members.

In January 2023, the CRI launched an International Counter Ransomware Task Force led by Australia. The ICTRF's objective is to share information about the actors and infrastructure conducting ransomware attacks and to support and accelerate member countries' disruption efforts. To do so, the ICTRF plans to develop research, findings and policy discussion into cross-sectoral tools, cyber threat intelligence exchanges, and collective best practice guidance for countering ransomware. The ICTRF will also act as a point of connection between the CRI and industry in relation to discussions about defensive and disruptive threat sharing and actions.

(b) **The Quad:** The Quadrilateral Security Dialogue, a partnership between the United States, India, Japan and Australia, has also focused on the coordination of cyber security responses. At the Quad Leaders' Tokyo Summit in 2022, the leaders of the Quad nations reaffirmed their intention to build resilience to cyber security vulnerabilities and cyber threats across the four nations, including by focusing on critical-infrastructure protection, supply-chain resilience and security, and software security standards. The Quad also agreed to strengthen information-sharing between computer emergency response teams, exchange best practice standards, and to improve software and Managed Service Provider security by coordinating cyber security standards for Quad governments' procurement of software.

(c) **AUKUS**: Through the trilateral security and technology pact, AUKUS, Australia has also been working with the US and UK to secure critical technologies, improve cyber coordination and share advanced capabilities.

These partnerships allow Australia to share cyber threat information, exchange model cyber security practices, compare sector-specific expertise, drive secure-by-design principles and coordinate policy and incident response activities with its international counterparts.

4.6 Future directions

Australia

Significant reforms in cyber security and data governance are likely to occur in Australia in the near future. As set out in the Strategy Paper, the Australian Government's objective is to make Australia the most cyber secure nation in the world by 2030. At this stage, it is not clear what reforms will result from the consultation in relation to the Strategy Paper.

In addition, significant new cyber security-related obligations are expected to be introduced under changes to Australia's data privacy arising out of the Attorney-General's landmark Privacy Act Review Report. Key changes which may be introduced include:

(a) introducing a direct right of action (both individual and representative proceedings) for breach of the *Privacy Act 1988 (Cth)*;

(b) introducing a maximum 72-hour period for notification of data breaches under the existing mandatory data breach notification scheme, and a requirement to notify individuals as soon as practicable;

(c) introducing a baseline set of information security outcomes that organisations will be required to achieve through application of reasonable technical and organisations measures; and

(d) significantly broadening the range of enforcement mechanisms, including removing the requirement for a breach to be 'serious or repeated' before a penalty is imposed.

There is currently no legislation in Australia that explicitly prohibits the payment of ransoms in relation to cyber security incidents, nor is there any legislation that requires Australian companies to report the making of ransomware payments to relevant authorities. It is possible that the Strategy Paper will recommend the introduction of legislation to one of those effects.

Comparator Jurisdictions

Similar significant new cyber security regulation developments are being pursued in the Comparator Jurisdictions.

In the US, the White House recently published its 2023 National Cyber security Strategy. Although the strategy does not particularise the proposed new cyber obligations, it sets out the US Government's intention to integrate federal cyber security centres, establish new critical infrastructure cyber security requirements, scale intelligence sharing and victim notification mechanisms. In addition, it proposes developing legislation establishing liability for software products and services, to prevent manufacturers and software publishers with

market power from fully disclaiming liability by contract, and to establish higher standards of care for software in specific high-risk scenarios.

In Canada, there are new obligations proposed for operators of critical cyber systems, as well as similarly significant new developments regarding the Canadian federal privacy framework. In particular, the Canadian federal government proposes to:

(a) create a new privacy related private right of action for affected individuals;

(b) overhaul the legislation governing companies' obligations with respect to personal information;

(c) establish an administrative tribunal to hear appeals of decisions made by the Privacy Commissioner of Canada and apply a new administrative monetary penalty regime; and

(d) regulate international and interprovincial trade and commerce in AI systems.

In the EU, on top of its already advanced cyber regulatory landscape, additional new and enhanced cyber obligations are proposed. Under the EU's proposed:

(a) *Cyber Resilience Act*, onerous obligations may be placed on certain companies to ensure a minimum standard of cyber security in relation to certain products with digital elements; and

(b) *AI Act*, some companies that provide 'high risk' AI systems may have specific obligations to:

  (i) establish a risk management system to identify and evaluate associated risks with the AI system as well as adoption of suitable risk management measures;

  (ii) adhere to data governance and management requirements, particularly for data used to train AI systems; and

  (iii) inform national authorities about serious incidents or malfunctions that constitute a breach of fundamental rights, as well as any recalls or withdrawals of AI systems from the market.

The UK's cyber regulatory landscape is also moving quickly. In particular, the UK Government has proposed amendments to the existing privacy and data protection regime under the *Data Protection and Digital Information Bill*. Notably, these amendments propose to increase the scope of the key regulator's enforcement power to include, for example, the power to compel companies to produce reports and attend interviews.

5. Results of Comparative Analysis

Attachment 1 sets out a summary table of our analysis of the laws of Comparator Jurisdictions across 3 dimensions:

- The existence of economy wide cyber security regulation;
- The existence of specific cyber security obligations applying to critical assets or systems of national significance; and
- The existence of significant sector or industry specific cyber security obligations.

Attachment 2 sets out our detailed comparison of cyber security obligations across Comparator Jurisdictions across the dimensions outlined in the scope of this review.

Cheng Lim & Nicola Charlston
Partners, King & Wood Mallesons

14 April 2023

Glossary

TERM	DEFINITION
ADI	Authorised Deposit-taking Institution (AU)
ACSC	Australian Cyber Security Centre
AFS	Australian Financial Services
AI	Artificial intelligence
AI Act	Proposal For a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts
AICD	Australian Institute of Company Directors
APP	Australian Privacy Principle
APRA	Australian Prudential Regulation Authority
ASD	Australian Signals Directorate
ASIC	Australian Security and Investment Commission
Bill C-26	*Bill C-26, An Act Respecting Cyber Security (CA)*
CCSPA	*Critical Cyber Systems Protection Act (CA)*
CCTX	Canadian Cyber Threat Exchange
CGC	UK Corporate Governance Code
CIRCIA	*Cyber Incident Reporting for Critical Infrastructure Act of 2022 (US)*
CIRMP	Critical Infrastructure Risk Management Program (AU)
CISA	Cyber security and Infrastructure Security Agency (US)
CiSP	Cyber Security Information Sharing Partnership
CJEU	Court of Justice of the European Union
Comparator Jurisdictions	Australia, United States (Federal), Canada, and the European Union
CPS 234	Prudential Standard CPS 234
CRI	Counter-Ransomware Initiative
CSE	Communication Securities Establishment (CA)
CSIRT	The National Computer Security Incident Response Team
DORA	*Regulation (EU) 2022/2554 on digital operational resilience for the financial sector*
DPA	*Data Protection Act 2018 (UK)*

TERM	DEFINITION
DPB	Data Protection and Digital Information Bill (UK)
DPO	Data Protection Officer
EBA	European Banking Authority (EU)
EECC	European Electronic Communication Code
EC Directive	Privacy and Electronic Communications Regulations 2003 (UK)
eIDAS Regulation	*Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (Electronic Identification, Authentication and Trust Services Regulation)*
ENISA	European Union Agency for Cyber security
EU-CyCLONe	Cyber Crisis Liaison Organisation Network
FCA	Financial Conduct Authority (UK)
FSMA	*Financial Services and Markets Act 2000 (UK)*
FTC	Federal Trade Commission (US)
FTC Act	*Federal Trade Commission Act 1914 (US)*
GCHQ	Government Communications Headquarters (UK)
GDPR	*General Data Protection Regulation (Regulation (EU) 2016/679)*
GLBA	*Gramm-Leach-Bliley Act (US)*
HIPAA	*Health Insurance Portability and Accountability Act (US)*
HHS	Department of Health and Human Services (US)
ICO	Information Commissioner's Office (UK)
ICT	Information and Communication Technology
ICTRF	International Counter Ransomware Task Force
KWM	King & Wood Mallesons
MSP	Managed service provider (UK)
NCSC	National Cyber Security Centre (UK)
NIS	*Network and Information Security Directive (Directive (EU) 2016/1148)*
NIS 2	*Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cyber security across the Union*
OAIC	Office of the Australian Information Commissioner
OCR	Office for Civil Rights (US)

TERM	DEFINITION
OES	Operator of Essential Service/s (EU; UK)
OPC	Privacy Commissioner of Canada
OSFI	Office of the Superintendent of Financial Institution (CA)
PECN	Public Electronic Communications Networks (EU)
PECS	Publicly Available Electronic Communications Services (EU)
PIPEDA	*Personal Information and Electronic Documents Act 2000 (Canada)*
PRA	Bank of England Prudential Regulation Authority
PS	Public Safety Canada
PSD2	*Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (Payment Service Directive 2)*
Quad	The Quadrilateral Security Dialogue between the United States, India, Japan and Australia
RDSP	Relevant Digital Service Provider
SEC	Securities and Exchange Commission (US)
SOCI Act	*Security of Critical Infrastructure Act 2018 (Cth)*
SON/s	System/s of National Significance (AU)
SPOC	National Single Point of Contact (EU)
Supervisory Statement	Supervisory Statement SS1/21 'Operational Resilience: Impact tolerances for important business services' (UK)
Strategy Paper	The 2023-2030 Australian Cyber Security Strategy Discussion Paper issued by the Expert Advisory Board appointed by the Australian Government
TSA	Transport Security Administration (US)
UK GDPR	*Regulation (EU) 2016/679 of the European Parliament and of the Council 2016 (UK)*
UK NIS	*The Network and Information Systems Regulations 2018 (UK)*
UK TSA	*Telecoms Security Act 2021 (UK)*
UK TSA Regs	*Electronic Communications (Security Measures) Regulations 2022 (UK)*

KING&WOOD MALLESONS

Attachment 1

Summary of Comparison of Cyber Security Obligations across Comparator Jurisdictions

	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA	EU	UK
1	**Pending or new developments in cyber security legislation**[11]					
		Significant new developments, including privacy reform and a new national cyber security strategy.	**Significant new developments**, including new regulations on security of critical infrastructure and cyber security reporting.	**Significant new developments**, including new obligations on operators of critical cyber systems, and changes to the federal privacy framework.	**Significant new developments**, including the implementation of NIS 2, DORA and the DORA Amending Directive by member states, as well as proposed acts on cyber resilience and AI regulation.	**Significant new developments**, including amendments to privacy legislation and upcoming amendments to UK NIS.
2	**Economy wide privacy obligations relating to cyber security**					
		Current federal legislation APP 11 of the Privacy Act requires agencies and organisations to take reasonable steps to protect the security of the personal information that they hold. However, the recent Privacy Act Review Report notes that reforms are needed to better align Australia's laws with global standards of information privacy protection to ensure sufficient cyber security.[12]	**No specific federal legislation regulating cyber security** The US does not have federal privacy legislation that requires the protection of personal information. Rather, privacy breaches are regulated through a general prohibition against 'unfair' practices.	**Similar to Australia** There is equivalent federal privacy legislation which requires the protection of personal information using appropriate security safeguards.	**More onerous obligations than Australia** The GDPR is the EU equivalent of the Australian Privacy Act. It imposes obligations to implement appropriate security measures to protect personal data and report data breaches.	**More onerous obligations than Australia** The DPA regulates how organisations process personal data. It incorporates the principles of the EU's GDPR, which is equivalent to the Australian Privacy Act. It imposes obligations to implement appropriate security measures to protect personal data and report data breaches.
3	**Specific cyber security obligations applying to critical assets or systems of national significance**					
		Current federal legislation The SOCI Act imposes specific cyber security obligations on responsible entities for critical infrastructure assets and SONs.	**Pending legislation** The US is in the process of developing regulations under CIRCIA that impose cyber incident reporting obligations on critical infrastructure entities. The objective of this legislation is comparable to that of the SOCI Act. However, as the scope of covered entities and cyber incidents has not yet been defined, it is still unclear whether the substance of the legislation will be comparable.	**Pending legislation** The Canadian Government has introduced a bill (Bill C-26) that will impose cyber security obligations on telecommunications service providers and operators of critical cyber systems. If introduced, the scope of this legislation will be similar to that under the SOCI Act.	**Similar to Australia** Under NIS, operators of essential services have obligations to detect and manage cyber security risks and notify relevant authorities where incidents occur. Further, under NIS 2, management bodies of regulated entities are expected to have the knowledge and skills to comprehend and assess cyber security risks and management practices, as well as their impact on the entity's services. These requirements are similar to those imposed by the SOCI Act.	**Scope of assets covered is narrower, no direct obligations on boards** UK NIS places specific cyber security obligations on organisations that operate essential services in a way similar to the SOCI Act, though the scope of covered assets is narrower (e.g. industries such as food and grocery, higher education and research and space technology do not appear to be covered). Further UK NIS does not directly impose cyber security obligations on boards of responsible entities. The UK has proposed to expand the scope of covered assets/industries.

[11] Please see section 11 of Attachment 2 for further details about the types of developments in each jurisdiction.

[12] Privacy Act Review Report, see 1, proposal 21.6, and [6.21].

	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA	EU	UK
4	**Prominent sector or industry specific cyber security obligations**	**Current federal regulation** The SOCI Act imposes specific cyber security obligations on responsible entities for critical infrastructure assets and SONS. There are also sector specific obligations in: • Telecommunications (under the Telecommunications Security Determination), and • financial services (CPS 234)	**Pending legislation - current legislation only covers a few select sectors** At this stage, the main sectors with specific cyber security obligations are the financial, health, rail and aviation sectors. The scope of sectors covered is narrower than that covered by the SOCI Act. However, as considered above, the US is in the process of developing regulations under CIRCIA that will impose obligations on critical infrastructure entities.	**Pending legislation - current legislation only covers a few select sectors** Current federal legislation only covers the telecommunications and financial sectors. However, there is pending legislation (Bill C-26) that will seek to impose cyber security obligations on operators of critical cyber systems including transportation systems and certain energy providers. However, even if Bill C-26 passes, fewer sectors are likely to be covered than those in the SOCI Act given provincial jurisdiction over a variety of industries in Canada.	**Similar to Australia** On top of the NIS frameworks, there is sector-specific legislation covering the financial, payments, and communications sectors. Additionally, the EU is also seeking to regulate artificial intelligence system providers through the proposed AI Act.	**Similar to Australia** Similarly to the SOCI Act, UK legislation applies specific obligations to providers of essential services such as electricity, telecommunications and health. Additionally, UK NIS also applies specific obligations on digital services providers such as providers of online marketplaces and cloud computing services. The *Telecommunications (Security) Act 2021 (UK)*, the Electronic Communications (Security Measures) Regulations and Telecommunications Security Code of Practice[13] are similar to, but more detailed and stringent than the equivalent Australian regulations. The guidance provided by the FCA in the UK for financial services firms is similar to that issued by ASIC in Australia.
5	**Reporting and notification obligations attaching to cyber security incidents**	**Current federal regulatory obligations** There are reporting obligations for cyber security incidents under: • The SOCI Act, • The Telecommunications Act, and • CPS 234.	**Pending legislation - current legislation only covers a few select sectors** Currently, only the HIPAA and the TSA Directives impose reporting and notification obligations in relation to cyber security incidents. However, this is subject to change once the scope of covered entities and reportable incidents are defined under CIRCIA.	**Similar to Australia, though reporting timelines are less stringent** The PIPEDA requires organisations to report cyber security incidents to the Office of the Privacy Commissioner, notify affected individuals, and keep records of breaches. However, unlike the SOCI Act, the legislation does not impose a strict reporting timeline. Bill C-26 would require "immediate" reporting of incidents affecting critical cyber systems, and OSFI requires federally-regulated financial institutions to report cyber incidents within 24 hours.	**More onerous obligations than Australia** Unlike the Australian Privacy Act (which employs a 'as soon as practicable' threshold), the GDPR requires all data controllers to, where feasible, report personal data breaches within 72 hours of becoming aware. Under the NIS frameworks, entities have obligations to notify relevant authorities 'without undue delay'. Certain entities also have obligations under sector-specific legislation such as the PSD2, the eIDAS Regulation, EECC and the e-Privacy Directive. These requirements are similar to those imposed by the SOCI Act and other sector-specific legislation. Notifications in respect of e-Privacy and eIDAS incidents must be made within 24 hours, not 72. The proposed AI Act also seeks to require providers of high-risk AI systems to inform authorities about serious incidents or malfunctions of AI systems. There is no AI-specific legislation currently proposed in Australia.	**More onerous obligations than Australia** As in the EU, the UK GDPR requires all data controllers to notify the Information Commissioner of personal data breaches within 72 hours. This is more onerous than the Australian Privacy Act's 'as soon as practicable' threshold. Under UK NIS, operators of essential services are required to disclose cyber security incidents to relevant authorities, also within 72 hours. Certain entities also have obligations under sector-specific legislation such as the Telecoms Security Act, UK eIDAS Regulation and the *Financial Services and Markets Act*. These requirements are similar to those imposed by the SOCI Act and other sector-specific legislation. For e-Privacy and UK eIDAS, notifications must be made within 24 hours, not 72.

[13] *Telecommunications (Security) Act 2021*; the Electronic Communications (Security Measures) Regulations 2022; Telecommunications Security Code of Practice

	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA	EU	UK
6	**Listed company disclosure obligations relating to cyber security incidents**	**ASX Listing Rules** Listed companies are required to disclose information, such as the occurrence of a cyber security breach that substantially impacts the price of their securities.	**Less stringent disclosure obligations than Australia** Unlike the requirement to 'immediately' disclose details of certain cyber incidents to the ASX, a public company is required to inform investors in a 'timely fashion'. Nevertheless, material incidents should still be reported as soon as possible as delays may result in derivative and/or securities lawsuits. Proposed amendments may enhance current requirements.	**Similar to Australia** Like in Australia, listed companies are required to disclose information, such as the occurrence of a cyber security breach that constitutes a material fact or a material change within the meaning of securities legislation, including if it substantially impacts the price of the company's securities.	**Similar to Australia** Like in Australia, listed companies in the EU are generally required to disclose inside information that could affect the price of their securities, such as the occurrence of a cyber security breach.	**Similar to Australia** Like in Australia, listed companies in the UK are required to disclose information, such as the occurrence of a cyber security breach that substantially impacts the price of their securities.
7	**Director duties relating to cyber security**	**General director duties** Directors have general duties of care, skill and diligence to their organisations under section 180 of the Corporations Act 2001 (Cth). This means that directors should be capable of satisfying themselves that cyber risks are adequately addressed and that organisations are cyber resilient.	**Similar to Australia** Like in Australia, directors owe fiduciary duties (including duties of care and loyalty) to shareholders. Directors and officers of public companies must ensure they exercise appropriate governance over cyber security risk, including by being properly informed about the relevant risks and the steps taken by the company to address such risks.	**Similar to Australia** Like in Australia, directors and officers of a corporation are required, in exercising their powers and discharging their duties, to exercise care, diligence and skill. This duty of care, diligence and skill is likely to extend to matters of cyber security.	**Similar to Australia** Local laws in Member States should be consulted where relevant as the general fiduciary duties of directors is a matter of national legislation in the European Union. Boards of certain listed companies must also ensure that their risk management frameworks are sufficient to identify and manage cyber risks and to ensure that they have systems in place to manage disclosures required to be made to the market.	**Similar to Australia** Like in Australia, directors have relevant duties under the UK Companies Act 2006, including a duty to exercise reasonable skill, care and diligence.
8	**Presence of direct rights of action or statutory tort arising out of a cyber security or data breach**	**No such rights** There are no direct rights of action or statutory torts related to a cyber security or data breach	**Similar to Australia** There are no direct rights of action or statutory torts related to a cyber security or data breach.	**Similar to Australia** There is no federal direct right of action or statutory tort related to cyber security or a data breach. PIPEDA does, however, provide a right to individuals to claim damages from an organization in Federal Court following an OPC investigation and report of findings or notice of discontinuance. Legislation is currently proposed to establish a direct right of action for individuals whose privacy is infringed.	**More advanced than Australia** There is a direct cause of action under the GDPR.	**More advanced than Australia** There is a direct cause of action under the UK GDPR.

	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA	EU	UK
9	**Class actions**					
		Limited scope for class actions There is currently limited scope for class actions relating to cyber breaches.	**Class actions more common than Australia** Class actions for cyber security breaches are increasingly common. Although there is no direct right of action or statutory tort arising out of a cyber security or data breach, actions are brought on grounds including breaches of express or implied contracts, negligence, other common law torts, breaches of securities laws, or breaches of consumer protection legislation.	**Class actions more common than Australia** Class actions for breaches of personal information are commonly brought. However, Canadian courts have been broadly sceptical about data breach class action claims. Legislation is currently proposed to establish a direct right of action for individuals whose privacy is infringed. If introduced, this may increase the scope for cyber breach related class actions.	**Greater scope for class actions than Australia** Data subjects have a direct right of action in the EU, which means there is greater scope for class actions than in Australia. Even more, there is a right to pursue class actions under the GDPR without the consent of the affected individuals.	**Greater scope for class actions than Australia** As in the EU, data subjects have a direct right of action in the UK, which means there is greater scope for representative actions than in Australia. However, the courts have not yet comprehensively determined this issue.
10	**Key cyber security regulator**					
		No overarching regulator - sector-specific regulators only While there is no single cyber security regulator, the Department of Home Affairs plays a very significant central and coordinating role because of its administration of the SOCI Act which covers many industry sectors. While the OAIC has an overarching role in relation to privacy and data breaches, there are also sector specific regulators for telecommunications and financial services	**No overarching regulator - sector-specific regulators only** Like Australia, there is no single cyber security regulator. The FTC acts in relation to information / privacy matters, the SEC acts in relation to financial institutions and listed entities, and the CISA (a component of the Department of Homeland Security) acts in relation to US critical infrastructure. Further, the HHS and OCR act in relation to the health sector.	**No overarching federal regulator - outside of privacy regulator, federal regulators have a limited role in cyber security and are sector-specific** Like Australia, there is no single cyber security regulator. The OPC regulates all organisations subject to PIPEDA. The financial regulator, OSFI, has issued guidance around cyber security risk and management, though it does not have an official role in cyber security regulation. Other industry-specific regulators are also involved (or may under pending legislation become involved) in cyber security regulation.	**No overarching regulator - country-specific regulators only** There is no overarching cyber security regulator in the EU, though there are a number of EU bodies with responsibilities in connection with EU laws relating to cyber security, such as the European Data Protection Board. Each member state will have its own system of regulators.	**ICO is the general cyber security regulator** The ICO is the overarching cyber security regulator. The ICO enforces the UK GDPR, e-Privacy as well as UK NIS and UK eIDAS regulation requirements. Other sector-specific regulators have powers within their competence, such as the PRA/FCA in the financial sector and Ofcom in relation to communications.
11	**Level of guidance and support the cyber security regulator provides industry**	Regulators in each jurisdiction have published a range of guidance materials on cyber security, including best practice guidelines and interpretation of the regulatory framework				
12	**Mechanisms or frameworks to facilitate the sharing of intelligence or support in the event of a significant cyber security incident**					
		There are federal institutions that support or facilitate intelligence sharing These include the CISC, the ACSC and CERT Australia.	**Similar to Australia** Like Australia, there are voluntary systems to share information about cyber security threats, incidents, vulnerabilities and defensive measures.	**Similar to Australia** Like Australia, there are voluntary systems to share information about cyber security threats, incidents, vulnerabilities and defensive measures.	**More advanced than Australia** There are many mechanisms and networks that facilitate the sharing of intelligence and collaboration in the EU, with further developments to be implemented under NIS 2.	**Similar to Australia** Like Australia, there are voluntary systems to share information about cyber security threats, incidents, vulnerabilities and defensive measures.

Attachment 2

Detailed Comparison of Cyber Security Obligations across Comparator Jurisdictions

#		REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
1	(a)	**Economy wide privacy obligations relating to cyber security**	Yes, Australian Privacy Principle 11 of the *Privacy Act 1988* (Cth)[15] requires agencies and organisations to take reasonable steps to protect the security of the personal information that they hold. While small business is exempt from this obligation there are reform proposals that would extend this obligation to all private sector organisations in Australia.	Yes, the *Federal Trade Commission Act 1914*[16] prohibits 'unfair' or 'deceptive' acts or practices that affects commerce.[17] The Federal Trade Commission, supported by the courts, has interpreted failing to implement reasonable data security measures as an 'unfair' practice.[18] [19]	Yes, Canada's federal private-sector privacy legislation, the *Personal Information Protection and Electronic Documents Act*[20], applies to private-sector organisations that collect, use or disclose personal information in the course of commercial activity. Only organizations operating in federally regulated industries must apply PIPEDA to employees' personal information. Principle 7 of PIPEDA's Fair Information Principles requires entities to protect personal information using appropriate security safeguards relative to the sensitivity of the information as well as the amount, distribution, and format of the information, and the method of storage.[21] Safeguards should include physical, technological and organizational measures. Organizations should also develop and implement a security policy, review safeguards regularly, exercise care in disposing of or destroying personal information, and ensure employees are adequately trained.[22] In Part 1 of Bill C-27, the *Digital Charter Implementation Act 2022*, Canada's federal government has proposed to replace PIPEDA with the *Consumer Privacy Protection Act*.[23] PIPEDA's safeguard requirements are, however,	Yes, the *General Data Protection Regulation (Regulation (EU) 2016/679)* imposes obligations on data processors and data controllers to implement appropriate security measures to protect personal data and report data breaches.[24] The GDPR also contains an accountability principle, which requires data controllers to be able to demonstrate compliance with the data processing principles.[25] This includes the principle that personal data shall be processed in a manner that ensures appropriate security of the personal data. [26]	Yes, the *Data Protection Act 2018* (UK)[27] incorporates the principles of the EU's GDPR into the UK's data protection regime as the *Regulation (EU) 2016/679 of the European Parliament and of the Council 2016* (UK).[28] As in the EU, data processors and data controllers must implement appropriate security measures to protect personal data and report data breaches.[29] The UK GDPR contains an accountability principle, which requires data controllers to be able to demonstrate compliance with the data processing principles.[30] This includes the principle that personal data shall be processed in a manner that ensures appropriate security of the personal data.[31]

[14] European Commission, 'Cyber security Policies'.
[15] *Privacy Act 1988* (Cth) (***Privacy Act***).
[16] *Federal Trade Commission Act 1914* (US) (***FTC Act***).
[17] FTC Act (US) s 5.
[18] *FTC v Wyndham Worldwide Corp* (2015) 799 F.3d 236.
[19] We note that Rule 10b-5 of the Securities and Exchange Act of 1934 may be indirectly applicable. Under Rule 10b-5, a company and its directors and officers may be held liable for misstatements or omissions of material fact that investors rely upon in their decision to buy or sell a security.
[20] *Personal Information Protection and Electronic Documents Act* (Canada), (S.C. 2000, c. 5).
[21] PIPEDA, Schedule 1, s. 4.7 (Principle 7).
[22] PIPEDA, Schedule 1, s. 4.7 (Principle 7); Office of the Privacy Commissioner of Canada (**OPC**), *Interpretation Bulletin: Safeguards* (June 2015).
[23] Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, Parliament of Canada.
[24] *General Data Protection Regulation (Regulation (EU) 2016/679)* (***GDPR***) arts 32, 33, 25, 28.
[25] GDPR art 5(2).
[26] GDPR art 5(1)(f).
[27] *Data Protection Act 2018* (UK) s 22(1) (***DPA***).
[28] GDPR arts 32, 33, 25, 28 as incorporated into UK law by section 3 of the Withdrawal Act 2018 (as amended) (***UK GDPR***); DPA ss 66, 67 and 68.
[29] UK GDPR arts 32, 33, 25, 28.
[30] UK GDPR, art 5(2).
[31] UK GDPR art 5(1)(f).

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
				expected to be maintained under the CPPA. Certain provinces (namely, Québec, British Columbia, and Alberta) are deemed by the federal government to have "substantially similar" privacy legislation. In those provinces, PIPEDA is displaced by the provincial private-sector privacy law for privacy matters within the province, other than in respect of federally regulated industries. These provincial laws also require the use of reasonable security safeguards. An entity operating across multiple provinces will often be subject both to relevant provincial privacy laws as well as PIPEDA. Moreover, Canada's federal *Privacy Act* applies to the federal public sector, including federal government departments, agencies and Crown corporations. The Act governs the federal government's collection, use, disclosure, retention and disposal of personal information and, by means of related directives and policies, requires appropriate safeguards to protect such information. All provinces and territories have similar laws governing their own public sectors.		
(b)	**Governance Implications**	APP 1.2 requires agencies and organisations to take reasonable steps to implement practices, procedures, and systems to ensure compliance with the APPs.[32] The Privacy Management Framework published by the Office of the Australian Information Commissioner sets out the following steps that entities are expected to take to comply with their obligations under APP 1.2: • ensure your leadership and governance arrangements create a culture of privacy that values personal information,	There are no direct duties on company directors in the FTC Act.	There are no direct duties on company directors in PIPEDA; however, Principle 1 of the PIPEDA Fair Information Principles, "accountability", dictates that an organisation is responsible for personal information under its control and shall designate an individual who is accountable for the organisation's compliance with PIPEDA's Fair Information Principles, including the safeguards requirement.[35] Directors also have relevant duties under the federal and provincial corporate laws, including a duty to exercise their powers and discharge their duties with a degree of care, diligence, and skill that a reasonably prudent person would exercise in comparable circumstances.[36]	There are no direct duties on company directors in the GDPR.[37] Local laws in Member States should be consulted where relevant as the liability of directors is a matter of national legislation in the European Union. The GDPR also requires that appropriate technical and organisational measures which are designed to implement data-protection principles in order to meet the requirements of the GDPR and the rights of data subjects.[38] A Data Protection Officer must also be appointed by public authorities or bodies or where certain types of processing activities are carried out. A DPO must, among other things, directly report to	There are no direct duties on company directors in the UK GDPR.[40] Directors have relevant duties under the UK Companies Act 2006, including a duty to exercise reasonable skill, care and diligence.[41] In the event of a data breach a director may face claims for breach of these duties, most likely through a derivative action. The DPA also states that a director, manager, secretary, officer, or person is guilty of an offence and liable for a breach if it is proven that the offence was committed with the consent or connivance of that individual (or where it is attributable to their neglect).[42] Such offences include the unlawful obtaining, disclosure or retention of personal data;

[32] *Privacy Act* schedule 1, APP 1.2.

[35] PIPEDA Schedule 1, s. 4.1 (Principle 1).

[36] *See, e.g.*, Canada Business Corporations Act (R.S.C., 1985, c. C-44), section 122.

[37] UK GDPR art 4.

[38] GDPR, art.25.

[40] UK GDPR art 4.

[41] UK Companies Act 2006, section 174.

[42] DPA s 198.

#		REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
			• develop and implement robust and effective practices, procedures and systems, • systematically examine the effectiveness and appropriateness of your privacy practices, procedures and systems to ensure they remain effective and appropriate, and • continually improve privacy processes and ensure responsiveness to new privacy issues.[33] Directors also have relevant duties under the *Corporations Act 2001*, including a duty to exercise their powers and discharge their duties with a degree of care and diligence that a reasonable person would exercise if they were a director in the corporation's circumstances.[34]			the highest management level of an organisation.[39]	the re-identification of de-identified personal data and the alteration of personal data to prevent disclosure to the data subject.[43] The UK GDPR also requires that appropriate technical and organisational measures which are designed to implement data-protection principles in order to meet the requirements of the GDPR and the rights of data subjects.[44] A DPO must also be appointed by public authorities or bodies or where certain types of processing activities are carried out. A DPO must, among other things, directly report to the highest management level of an organisation.[45]
2	(a)	**Specific cyber security obligations applying to critical assets or systems of national significance**	Yes, SOCI Act[46] imposes obligations on responsible entities for critical infrastructure assets and Systems of National Significance to: • report ownership and operational information to the Government, • notify regulators of cyber security incidents within periods that range from 12 to 72 hours; depending on the criticality of the incident, • have and implement a risk management program that manages the 'material risk' of a 'hazard' occurring, which could have a relevant impact on the critical infrastructure asset. The hazards that have to be managed include but are not limited to	Yes, the *Cyber security and Infrastructure Security Agency Act 2018*[47] created the Cyber security and Infrastructure Security Agency, a federal agency responsible for protecting critical infrastructure in the United States.[48] The *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, requires CISA to develop and implement regulations requiring covered entities to report certain cyber incidents and ransomware payments to the CISA. Under CIRCIA, covered entities must report:[49] • certain cyber incidents to CISA within 72 hours after they have a reasonable belief the incident has occurred, and	No, there is currently no federal cyber security legislation that applies specifically to critical infrastructure in Canada. **Cyber security guidance by PS and CSE** Public Safety Canada is responsible for coordinating the departments and government agencies that play a role in ensuring cyber security for critical infrastructure and operators of essential services. It is the policy lead for cyber security within the federal government. The Communications Security Establishment, Canada's cryptologic agency, is Canada's technical authority for cyber security. Through its Canadian Centre for Cyber Security, and alongside PS, CSE works to provide support, advice and guidance on cyber security to	Yes, the *Network and Information Security Directive (Directive (EU) 2016/1148)* is currently the main legislation dealing with the cyber security of critical infrastructure. It requires member states to adopt and publish certain local cyber security laws. The current iteration of the directive will be repealed and replaced by the *Directive on measures for a high common level of cyber security across the Union (Directive (EU) 2022/2555*, which entered into force on 16 January 2023 and which must be adopted by member states by 17 October 2024.[53] **NIS** NIS applies to both 'digital service providers' (i.e. online marketplaces, online search engines and cloud	Yes, the *Network and Information Systems Regulations 2018 (UK)* imposes obligations on operators of essential services, which are entities that provide essential services into various energy, transport, health, water and digital infrastructure sub-sectors where those services rely on network and information systems and satisfy the relevant threshold requirement for the type of service in question.[55] Notably, providers of public electronic communications networks and services are not currently covered by the regulation given that they are regulated under the Communications Act 2003 (see section 3 below). Under the UK NIS, OESs are required to:

[33] OAIC, 'Privacy Management Framework: enabling compliance and encouraging good practice' (2015).

[34] Corporations Act 2001 s 180(1) (***Corporations Act***).

[39] GDPR, arts. 37, 38 and 39.

[43] UK Data Protection Act 2018 sections 170 to 173.

[44] UK GDPR, art.25; DPA, ss 55, 56, 57 and 59.

[45] UK GDPR, arts. 37, 38 and 39; DPA, ss 69, 70 and 71.

[46] *Security of Critical Infrastructure Act 2018* (Cth) (***SOCI Act***).

[47] *Cyber security and Infrastructure Security Act 2018* (US).

[48] *Cyber security and Infrastructure Security Act 2018* (US).

[49] *Cyber Incident Reporting for Critical Infrastructure Act of 2022* s 2242.

[53] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cyber security across the Union (***NIS 2***), which is preceded by Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (***NIS***). NIS 2 entered into force on 16 January 2023, and member states are required to transpose the Directive into national legislation by 17 October 2024 (which is when the majority of obligations will come into force). NIS will continue to apply until 18 October 2024. For more detail see, 'NIS 2 Directive – now is the time to act', Fieldfisher.

[55] *The Network and Information Systems Regulations 2018* (UK) s 8(1) (***UK NIS***).

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
		cyber security risks, supply chain and personnel risks, and • comply with directions from Government in relation to an actual or anticipated cyber security incident. The sectors of critical infrastructure that are covered by the SOCI are: • communications, • data storage and processing, • defence industry, • energy, • financial services and markets, • food and grocery, • health care and medical, • higher education and research, • space technology, • transport, and • water and sewerage. In the case of a SON, entities must comply with enhanced cyber security notifications. These include: • developing cyber security incidence response plans, • undertaking cyber security exercises, • undertaking vulnerability assessments, and • providing systems information in near real time.	• report a ransomware payment as a result of an attack against the covered entity within 24 hours of payment. However, at this stage, the scope of covered entities and covered cyber incidents have not yet been defined. CIRCIA will not take effect until the CISA publishes a Final Rule establishing these definitions. Note that the director of CISA must publish proposed rules in the form of a Notice of Proposed Rulemaking no later than March 2024, and the Final Rule must be published no later than September 2025. The National Cyber Security Strategy recently published by the Biden Administration indicates that security of critical infrastructure is one of the Federal Government's key focuses, with the strategy focusing on establishing new cyber security requirements in key sectors such as oil and gas, aviation, rail, and water systems.[50]	Canada's critical infrastructure operators. CSE is mandated under the *Communications Security Establishment Act* to provide these services.[51] **Proposed cyber security obligations under Bill C-26** On 14 June 2022, the Canadian government introduced Bill C-26. [52] If passed, Part 1 of Bill C-26 would amend Canada's *Telecommunications Act* to implement new cyber security obligations for telecommunications service providers, including providing the government with powers to order such providers to take action or refrain from acting in order to mitigate or remedy cyber security risks. If passed, Part 2 of Bill C-26 would enact the *Critical Cyber Systems Protection Act*, which would impose cyber security obligations on designated operators of any "critical cyber system". "Critical cyber system" is defined as any cyber system that, if compromised, could affect the continuity or security of a "vital system" or "vital service". Schedule 1 of the draft Bill defines vital services or systems to include: • banks, • telecommunications services, • interprovincial or international pipeline and power line systems, • transportation systems, • nuclear energy system, and • clearing and settlement systems If Bill C-26 is passed, designated operators would have an obligation to: • create, implement and maintain a cyber security program meeting a number of safeguards, • notify relevant regulators of their cyber security program,	computing services) and 'operators of essential services', i.e. specified entities operating within the following sectors: • energy, • transport, • banking, • financial market infrastructures, • health, • water supply and distribution, and • digital infrastructure.[54] Notably, NIS does not apply to telcos or payment service providers, who are subject to separate security and incident reporting obligations, or to hardware / software developers. Under NIS, entities are required to: • put in place appropriate and proportionate technical and organisational measures to detect and manage risks posed to the security of the network and information systems on which their services rely, and • notify the relevant authority about incidents that have a 'significant impact' on the continuity of core services provided. **NIS 2** NIS 2 builds on NIS. However, in acknowledgment of the fact that network and information systems have become an integral part of services provided by a far wider range of industries than was the case in 2016, it reflects a considerable broadening of scope versus NIS. NIS 2 applies to all entities which: (i) provide their services or carry out their activities in the EU; (ii) meet or exceed the thresholds to qualify as medium-sized enterprise (i.e. employ more than	• take appropriate and proportionate technical and organisational measures to detect and manage risks posed to the security of the network and information systems on which their services rely, and[56] • notify the designated competent authority about any incident which has a significant impact on the continuity of the essential services.[57] Relevant digital service providers, such as those that provide online marketplaces, online search engines or cloud computing services, [58] must also take additional steps under the UK NIS. For example, they must notify the Information Commissioner about any incident having a substantial impact on these services within 72 hours.[59] • Following a consultation in 2022, the UK Government announced its intention to update UK NIS to improve the UK's cyber resilience. The proposed changes include: • bringing managed service providers into scope of UK NIS to keep digital supply chains secure, • improving cyber incident reporting to regulators such as Ofcom (communications), Ofgem (energy) and the ICO (privacy), • establishing a cost recovery system for enforcing UK NIS, • giving the government the power to amend UK NIS in future to ensure it remains effective, and • enabling the Information Commissioner to take a more risk-based approach to regulating digital services.

[50] *National Cyber security Strategy* (Report, March 2023).

[51] *Communications Security Establishment Act* (S.C. 2019, c. 13).

[52] Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, Parliament of Canada.

[54] See 'NIS Directive establishes first EU-wide cyber security rules', Fieldfisher.

[56] UK NIS s 10.

[57] UK NIS s 11.

[58] UK NIS s 12(1).

[59] UK NIS s 12(6)(a).

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
				• mitigate supply-chain and third-party risks, • report cyber security incidents to CSE, • comply with and maintain the confidentiality of directions received pursuant to the Act, and • keep records related to the above.	50 employees and have an annual turnover and/or annual balance sheet total exceeding EUR 10 million); and (iii) operate in one of the following sectors (in addition to all those sectors covered by NIS): • food production, processing and distribution, • manufacturing, • postal and courier services, • additional categories of digital infrastructure including providers of public electronic communications networks or services, trust service providers, data centre service providers, and content delivery network providers (these are now in scope of NIS 2, as distinct from NIS), • ICT service management, • waste water and waste management, • public administration, • space, • research, and • chemicals. Within each of these broad industry sectors, NIS 2 specifies the relevant subsectors which are within scope. Whilst some of these subsectors were previously caught by NIS, others are entirely new (e.g. in the energy sector, the district heating and cooling and hydrogen subsectors have been added). There is a further differentiation in NIS 2 between “essential entities” and “important entities”, with different regimes under NIS 2 applying to each. (Identifying which specific organisations will fall within each bucket has to some extent been left to Member States). NIS 2 sets out new cyber security incident reporting rules. It requires any incident with a ‘significant impact’ on in-scope services to be notified to national computer security incident response teams or regulators within tight timeframes. These are incidents that have: • caused, or are capable of causing, severe operational disruption of the services, or • affected, or are capable of affecting, other natural or legal	

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
					persons by causing considerable material or non-material damage. NIS 2 also bolsters the obligations under NIS by requiring all in-scope entities to implement a core set of cyber security risk management measures, that cover risk analysis and information system security policies, incident handling protocols, business continuity plans, encryption and cryptography, testing and auditing procedures, vulnerability disclosure, cyber security training and ICT supply chain security. It also introduces enhanced sanctions for breach of the cyber security risk management and reporting obligations, and imposes responsibility directly on management for compliance.	
(b)	**Governance implications**	As a general rule, the Board of an entity that is responsible for a critical infrastructure asset (including a SON) under the SOCI Act will be responsible for oversight of compliance with those obligations. A failure to do so could give rise to liability on the part of directors under the Australian Security and Investment Commission's 'stepping stones' approach to liability.[60] More directly, the SOCI Act does require the Board of a responsible entity to approve an annual report that the entity is required to provide to the Department of Home Affairs that states whether the risk management program was up to date, any variations to the program, and details of how the program was effective in mitigating any relevant impacts that hazards may have had on that asset during that year. This will necessarily require the Board to satisfy itself as to the adequacy of the risk management program. The SOCI Act has a fixed civil penalty of 50 penalty units for any contravention. This is equal to AUD $13,750 at the current value of a penalty unit.[61]	As CISA is still in the process of developing the relevant regulations under CIRCIA, there are no governance implications that relate specifically to boards of entities responsible for critical infrastructure assets at this stage.	The proposed CCSPA does not impose any specific obligations on the Board of a designated operator. However, under the proposed Bill, if a designated operator commits a violation or an offence under the Act, any director or officer of the designated operator who directed, authorised, assented to, acquiesced in or participated in the commission of the offence is a party to the offence and can be held liable (even if the designated operator is not prosecuted for or convicted of the offence).[62] Regulators will have the power to issue administrative monetary penalties of up to CAD $1 million per day for individuals (such as directors and officers) and CAD $15 million per day in any other case.[63] Directors and officers may also be fined (in an amount at the discretion of the court) or imprisoned (for up to five years) if they are convicted of committing an offence under CCSPA.[64]	Under Article 20 of NIS 2, member states must ensure that the management bodies (i.e. boards and directors) of regulated entities approve and oversee the implementation of cyber security risk management measures. This means that management bodies are expected to have the knowledge and skills to comprehend and assess cyber security risks and management practices and their impact on the entity's services and are expected to undertake regular training in this space. Failing to maintain adequate risk oversight can expose companies, officers and directors to liability. Depending on the relevant breach and whether the entity is considered "essential" or "important", member states are required to provide for a maximum fine of up to €10,000,000 or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. In addition, for "essential entities", competent authorities can in some serious cases even impose a temporary prohibition on the exercise of managerial functions by CEOs / general counsel.	As distinct from NIS 2, there are currently no governance implications that relate specifically to boards of entities responsible for critical infrastructure assets under UK NIS at this stage. Furthermore, under UK NIS officers and directors of subject entities are not directly exposed to liability. Nor does this seem to be proposed as part of the draft package of reforms to NIS 2 mentioned in row 2(a) above. Depending on the relevant breach, penalty notices served under UK NIS must:[65] • not exceed £1,000,000 for any contravention which the enforcement authority determines was not a material contravention, • not exceed £8,500,000 for a material contravention which does not satisfy the below criteria, and • not exceed £17,000,000 for a material contravention which has or could have created a significant risk to, or impact on, the service provision by the OES or RDSP.

[60] *Australian Securities and Investments Commission v Vocation Limited* (in liquidation) [2019] FCA 807.

[61] Department of Infrastructure, Transport, Regional Development and Communications, ' Systems of National Significance regulatory reforms - Regulation Impact Statement', (June 2022) 3.

[62] Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, Part 2 (CCSPA), ss 93 and 138, Parliament of Canada.

[63] Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, Part 2 (CCSPA), ss 90, 91 and 93, Parliament of Canada.

[64] Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, Part 2 (CCSPA), ss 137 and 138, Parliament of Canada.

[65] UK NIS s 18(6).

#		REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
3	(a)	**Prominent sector or industry specific cyber security obligations**	**Financial sector** APRA The Australian Prudential Regulation Authority has issued Prudential Standard CPS 234 that sets out information security requirements that apply to all APRA regulated entities. These include authorised deposit-taking institutions, general insurers, life companies, friendly societies, private health insurers and registrable superannuation entities. CPS 234 requires regulated entities to: • clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals, • maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity, • implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls, and • notify APRA of material information security incidents. ASIC ASIC is Australia's integrated corporate, markets, financial services and consumer credit regulator. It has taken a very public position that Australia's financial markets and systems to be resilient to cyber incidents. While there are no specific obligations in Australian companies legislation dealing with cyber security ASIC recently successfully took	**Financial sector** The *Gramm-Leach-Bliley Act* regulates financial institutions' use, disclosure, and safeguarding of consumers' non-public personal information.[67] In particular, the GLBA and its implementing regulations require financial institutions to implement policies and procedures reasonably designed to ensure the security and confidentiality of customer records, and to protect against anticipated threats and unauthorised access and use. In March 2023, the SEC published a proposed rule requiring broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents to: • implement policies and procedures to address cyber security risks, • review and assess the design and effectiveness of such policies and procedures annually (including to ensure that they reflect changes in cyber security risk), • immediately notify the SEC where there is reasonable basis to conclude that a significant cyber security incident has occurred or is occurring, and • make public disclosures about (1) cyber security risks that could materially affect the entity's business and operations (including how the entity assesses, prioritises and addresses those risks), and (2) significant cyber security incidents that it has been affected by in the current or previous calendar year	**Financial sector** Under the *Bank Act 1991*, Canadian banks are required to establish procedures for safeguarding and restricting the retention, use and disclosure of personal financial information.[72] Financial service regulators have also published various guidelines and recommendations relating to cyber security. For example, the Office of the Superintendent of Financial Institutions' Technology and Cyber Risk Management Guideline sets out the regulator's expectations related to technology and cyber risk management in relation to federally regulated financial institutions, including banks, most insurance companies and federal pension plans. OSFI has also issued a Technology and Cyber Security Incident Reporting Advisory mandating incident reporting in certain circumstances. Likewise, the Investment Industry Regulatory Organisation of Canada has published a guide on cybersecurity best practices and implemented rules requiring its dealer members to report cyber security incidents.[73] **Telecommunications** Amendments to the Telecommunications Act The *Telecommunications Act*, including decisions and policies of the Canadian Radio-television and Telecommunications Commission adopted pursuant to the Act, require telecommunications service providers to protect the privacy of their users. As noted above, Bill C-26 would amend the *Telecommunications Act* to implement new cyber security protections for telecommunications service providers in Canada. The Bill grants the Minister Of Industry the power to direct telecommunications service providers to do anything or	The *Digital Operational Resilience Act* and DORA Amending Directive have entered into force and will apply in relation to financial entities from 17 January 2025. [76] The Regulation builds on ICT risk management requirements for financial organisations and seeks to harmonise the currently fragmented rules on operational resilience across the EU. The Regulation covers financial entities as well as ICT third-party service providers and introduces certain obligations, such as requiring financial institutions to maintain an ICT risk management framework, use updated ICT systems and introduce ICT security strategies and policies. In addition, financial entities must introduce an ICT-related incident management procedure and must report any major ICT-related incident to their relevant competent authority. Note that the NIS 2 provisions on cyber security risk-management and reporting, supervision and enforcement, do not apply to financial entities covered by DORA.[77] **Payment Service Providers** Payment Service Directive 2[78] PSD2 requires payment service providers to comply with additional cyber security obligations. These include implementing appropriate security policies and procedures, notifying major operational or security incidents without undue delay to the competent authority and notifying payment service users where incidents may have an impact on their financial interests, and performing annual risk assessments. Strong customer authentication must also be implemented in accordance with	**Financial sector** The UK will not be subject to DORA, however, the Bank of England Prudential Regulation Authority issued Supervisory Statement SS1/21 'Operational Resilience: Impact tolerances for important business services' in March 2021 (in force on 31 March 2022).[92] The Supervisory Statement applies to banks and insurers, including building societies and PRA-designated investment firms. It sets out the PRA's expectations for boards in relation to the operational resilience of firms' important business services including: • approve the important business services identified for their firm and the impact tolerances set for each, • regularly review the firm's important business services, • ensure they have the appropriate management information in relation to operational resilience, • collectively possess adequate knowledge, skills and experience to provide constructive challenge to senior management and inform decisions that have consequences for operational resilience.[93] The Financial Conduct Authority is the regulator for financial service firms and markets in the UK. It has issued guidance for all firms subject to the financial crimes rules on how it assesses a firm's governance approach to data security. [94] FCA sets out a number of examples of 'good practice' governance in relation to data security including: • having a clear figurehead championing the issue of data security,

[67] S. 900, Public Law 106-102 – Gramm-Leach-Bliley Act.

[72] *See, e.g., Bank Act*, S.C. 1991, c. 46, s 244.

[73] *See, e.g.*, Compliance with IIROC's Cyber security Incident Reporting Requirements, GN-3700-22-001, Feb. 10, 2022.

[76] Regulation (EU) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA). Directive (EU) 2022/2556 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector (***DORA Amending Directive***).

[77] NIS 2 recital 28.

[78] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (***PSD2***). For more detail see, Practical Law Financial Services, 'Overview of PSD2', Thomson Reuters.

[92] Bank of England, Prudential Regulation Authority, 'Operational Resilience: Impact tolerances for important business services', Supervisory Statement SS1/21, (March 2021) (***Supervisory Statement***).

[93] Supervisory Statement at [7.1]-[7.2].

[94] Financial Conduct Authority, *Financial Crime Guide: A firm's guide to countering financial crime risks* (Guide, February 2023) FCG 5 (***FCA Guide***).

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
		action against an Australian financial services licensee for breaching section 912A of the *Corporations Act 2001 (Cth)*[66] for failing to: • ensure adequate cyber security measures were in place and/or adequately implemented across its authorised representatives, and • implement adequate cyber security and cyber resilience measures and exposing its authorised representative's clients to an unacceptable level of risk. **Telecommunications** The Telecommunications (Carriage Service Provider—Security Information) Determination 2022 effectively applies certain of the obligations under the *SOCI Act* to carriers and carriage service providers in the telecommunications sector. These include the obligation to: • notify the Australian Signals Directorate of cyber security incidents within periods that range from 12 to 72 hours, depending on the criticality of the incident, and • report ownership and operational information to Government. **Critical infrastructure** The SOCI Act applies to 11 critical infrastructure sectors including communications, data storage or processing, defence industry, energy, financial services and markets, food and grocery, health care and medical, higher education and research, space	(including information about the persons affected, whether data was stolen, altered or accessed for unauthorised purposes, and the effect of the incident on the entity's operations).[68] At the date of writing, the SEC has not yet published the proposing release. **Health sector** The *Health Insurance Portability and Accountability Act* outlines the lawful use and disclosure of protected health information in the United States. This applies to most health care providers, health plans, and their service providers.[69] The HIPAA Security Rule, a related regulation, requires covered entities to implement data protection policies and reasonable security procedures. In particular, entities are required to implement technical safeguards such as authentication controls and encryption technology, which protect data and control access. **Transport** Transport Security Administration Security Directives (rail and aviation) Under Security Directive 1580-21-01A issued by the TSA, owners and operators of passenger and freight railroad carriers are required to develop and report on measures to improve cyber security resilience and prevent disruption and degradation to infrastructure. In particular, owners and operators are required to: • designate a Cyber security Coordinator who will serve as a principal point of contact with	refrain from doing anything that is necessary to secure the Canadian telecommunications system. Among other things, the Minister's order may: • prohibit providers from using any specified product or service in or in relation to the providers' network or facilities, or part thereof, • prohibit or impose conditions on service agreements for any product or service or with a specified person, • require providers to terminate a service agreement, • prohibit the upgrade of any specified product or service, • require providers to develop a security plan in relation to their services, networks or facilities, conduct assessments and/or mitigate vulnerabilities, and • subject the providers' networks, facilities and procurement plans to a review process.[74] Additionally, the Canadian Security Telecommunications Advisory Committee has published several guidance and best practice documents, including the Critical Infrastructure Protection Standards and the Security Incident Response Standard for Canadian Telecommunications Service Providers. **Other industries** Certain other industries, such as pipelines, are subject to more general security management requirements that can be read to extend to cyber security safeguards.[75] In addition, some industries, such as the healthcare sector,	regulatory technical standards in defined circumstances.[79] Note, however, that Article 19 is to be deleted in October 2024, and NIS 2 will instead apply. **Telecommunications** European Electronic Communication Code[80] Under Article 40 of the EECC, member states must ensure providers of public electronic communications networks and publicly available electronic communications services: • take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to security of networks and services,[81] • notify the competent authority without undue delay of a security incident that has had a significant impact on the operation of networks or services, and • inform their users potentially affected by a particular and significant threat of a security incident of any possible protective measures or remedies the users can take and, where appropriate, inform users of the threat itself.[82] As public electronic communications networks and publicly available electronic communications services will be brought within the scope of NIS 2, the above EECC requirements will be deleted with effect from 18 October 2024.	• clear plans to respond to data loss incidents and notify affected customers, • monitoring of accounts following a data loss to spot unusual transactions, and • looking at outsourcers' data security practices before doing business.[95] Regulated firms are expected to: • conduct their business with due care, skill and diligence,[96] • report material cyber incidents in accordance with the obligation to deal with regulators in an open and cooperative way,[97] and • take reasonable care to establish and maintain such systems and controls for compliance with regulatory requirements and standards and for countering the risk of financial crime.[98] Other principles apply in specific areas like pensions.[99] **Payment Service Providers** Payment Services Regulations 2017 PSD2 requires payment service providers to comply with additional cyber security obligations. These include implementing appropriate security policies and procedures, notifying major operational or security incidents without undue delay to the competent authority and notifying payment service users where incidents may have an impact on their financial interests, and performing annual risk assessments. Strong customer authentication must also be

[66] Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496.

[68] Securities and Exchange Commission, 'SEC Proposes New Requirements to Address Cyber security Risks to the US Securities Markets'; Securities and Exchange Commission, 'Cyber security Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents', (Proposed Rule, March 2023).

[69] H.R. 3103, Public Law 104 - 191 - Health Insurance Portability and Accountability Act of 1996 (***HIPAA***).

[74] Bill C-26, an Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, Part 1, s 15.2(2), Parliament of Canada.

[75] *See, e.g.*, Canadian Energy Regulator Onshore Pipeline Regulations, SOR/99-294, ss. 6.5, 47.1.

[79] PSD2, arts.5, 95, 96, 97, 98.

[80] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (***EECC***).

[81] EECC art 40(1).

[82] EECC art 40(3).

[95] FCA Guide [5.2.1].

[96] FCA Principles of Business, Chapter 2. Rule 2.1.1(2) (***PRIN2***); See also

[97] FCA Principles of Business, Chapter 2. Rule 2.1.1(11) (***PRIN11***).

[98] FCA Handbook, SYSC3.2.6.

[99] See Cyber security principles The Pensions Regulator | The Pensions Regulator.

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
		technology, transport and, water and sewerage.	TSA and CISA for cyber security-related matters, • report cyber security incidents to CISA, • develop a Cyber security Incident Response Plan, and • conduct a cyber security vulnerability assessment.[70] In March 2023, the TSA announced a new cyber security amendment that will extend the cyber security measures applying to rail operators to airport and aircraft operators. The TSA's announcement noted that under the forthcoming amendment, TSA-regulated entities must proactively assess the effectiveness of cyber security measures, including by: • developing network segmentation policies and controls to ensure that operational technology systems can continue to safely operate in the event that an information technology system has been compromised, and vice versa, • creating access control measures to secure and prevent unauthorized access to critical cyber systems, • implementing continuous monitoring and detection policies and procedures to defend against, detect, and respond to cyber security threats and anomalies that affect critical cyber system operations, and • reducing the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers and firmware on critical cyber systems	are ubjectt to provincial legislation and regulation.	e-Privacy Directive[83] The e-Privacy Directive (as amended) concerns the processing of personal data and the protection of privacy in the electronic communications sector in the EU. It is separate from the GDPR. Under Article 4 of the e-Privacy Directive, member states must implement the security of processing obligations set out below. (**Security measures**) Providers of PECSs must take appropriate technical and organisational measures to safeguard the security of their services with respect to network security. At a minimum, the technical and organisational measures must: • ensure that personal data can be accessed only by authorised personnel for legally authorised purposes, • protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and • ensure the implementation of a security policy with respect to the processing of personal data.[84] (**Personal data breach notification**): Providers of PECS shall, in the case of a personal data breach, without undue delay, notify: • the personal data breach to the competent national data protection authority, and • the relevant subscribers or individuals, when the personal data breach is likely to adversely affect their personal data or privacy.[85]	implemented in defined circumstances.[100] **Telecommunications** The Privacy and Electronic Communications Regulations 2003 apply to providers of a public electronic communications service and requires them to take appropriate technical and organisational measures to safeguard the security of that service.[101] The service provider must notify a personal data breach to the Information Commissioner without undue delay (and within 24 hours after detection, where feasible[102]) and must notify subscribers or users without undue delay if the personal data breach is likely to adversely affect their personal data or privacy.[103] • The UK has also recently implemented changes in the UK's security regime in the Communications Act 2003 by virtue of the Telecoms Security Act 2021 (UK TSA), the Electronic Communications (Security Measures) Regulations 2022 (UK TSA Regs), the Huawei Designated Vendor Direction and the Telecoms Security Code of Practice 2022. In summary, providers of public electronic communications networks and public electronic communications services must take measures as are appropriate and proportionate for the purposes of identifying and reducing the risks of and preparing for the occurrence of security compromises, • take reasonable and proportionate steps to bring relevant information of significant risks of security compromises to the attention of users who may be

[70] US Department of Homeland Security, *Security Directive 1580-21-01A*, (24 October 2022).

[83] Directive (EU) 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (***e-Privacy Directive***).

[84] E-Privacy Directive art 4.

[85] E-Privacy Directive art 4, as amended by Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States art 2(4) (***Citizens' Rights Directive***).

[100] Payment Services Regulations 2017, ss.98, 99, 100

[101] *The Privacy and Electronic Communications (EC Directive) Regulations 2003* (UK), s 5(1) (***PECR***).

[102] Commission Regulation (EU) No 611/2013, as incorporated into UK law.

[103] PECR, reg.5A.

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
			in a timely manner using a risk-based methodology. However, as the relevant Directive has not yet been published, the specific details of the measures are not yet clear.[71]		Electronic Identification, Authentication and Trust Services Regulation[86] This regulation applies to electronic trust services relating to the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals.[87] Article 19 introduces the following obligations concerning security measures and incident reporting for trust services: • providers of electronic "trust services" must implement appropriate technical and organisational measures for the security of the trust services that they provide,[88] • trust service providers must notify competent supervisory bodies and other relevant authorities within 24 hours of becoming aware of any security breaches that have a significant impact on the trust service provided or on the personal data maintained in it. Individuals must also be notified without undue delay where they are likely to be adversely affected by the breach,[89] and • where appropriate, national supervisory bodies must inform supervisory bodies in other EU countries and European Union Agency for Cyber security about security breaches.[90] As electronic trust providers will be brought within the scope of NIS 2, article 19 of the eIDAS Regulation will be deleted from 18 October 2024 but NIS 2 will retain the 24 hour notification period for trust service providers derived from article 19 of the eIDAS Regulation.	adversely affected by the security compromise, • inform Ofcom (the communications regulator) as soon as reasonably practicable of particular security compromises, • take appropriate and proportionate measures to protect data and network functions, and • comply with a range of other specific requirements, which range from removing Huawei equipment from network and services that are subject to the Huawei Designated Vendor Direction through ensuring that tools for monitoring or analysis are not capable of being accessed in or stored on equipment located in Iran, North Korea, PRC, or Russia. The TSA Code sets out a range of measures which Tier 1 providers (public telecoms providers with relevant turnover of £1bn or more) and Tier 2 providers (public telecoms providers with relevant turnover of more than or equal to £50m but less than £1bn) are expected to comply with over a range of different time periods for different measures starting between 2024 and 2028. The Product Security and *Telecommunications Infrastructure Act 2022* also creates cyber security obligations for UK manufacturers of connectable ('smart') products. The Act requires manufacturers, importers and distributors to investigate, take action on, and record cyber security incidents.[104] The eIDAS Regulation, which applies to providers of trust services, has been incorporated into UK law in amended form and therefore: • providers of electronic trust services established in the United

[71] Transport Security Administration, 'TSA issues new cyber security requirements for airport and aircraft operators', (7 March 2023).

[86] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (***eIDAS Regulation***).

[87] eIDAS art 3(12).

[88] eIDAS art 19(1).

[89] eIDAS art 19(2).

[90] eIDAS art 19(2).

[104] *Product Security and Telecommunications Infrastructure Act 2022* chapter 2.

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
					Artificial Intelligence EU Artificial Intelligence Regulation[91] The AI Act is a proposed law that will regulate all AI systems with an element of autonomy. As part of the proposed framework, some AI systems will be classified as 'high-risk', including AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic and the supply of water, gas, heating and electricity. Other prescribed 'high risk' systems include (among others) those used for certain purposes in education and vocational training, law enforcement, the provision of essential services, migration and border control, and the justice or democratic systems. AI systems that are used for a prescribed 'high risk' purpose under the proposed AI Act will be subject to a number of cyber security requirements, including: • the establishment of a risk management system to identify and evaluate associated risks, • adoption of suitable risk management measures, • adherence to data governance and management requirements (particularly for data used to train AI systems), and • designing the systems to have an appropriate level of accuracy, robustness and cyber security.	Kingdom must implement appropriate technical and organisational measures for the security of their activities, • trust service providers must notify the data protection authority within 24 hours of becoming aware of any security breaches that have a significant impact on the trust service provided or on the personal data maintained in it. Individuals must also be notified without undue delay where they are likely to be adversely affected by the breach.[105] (Cooperation by supervisory authorities with ENISA is not required under the UK eIDAS Regulation).
(b)	**Governance implications**	As for the SOCI, Act see above. **Financial sector** CPS 234 requires boards of regulated entities to be ultimately responsible for cyber security of the entity. It states that: • the board must ensure that the entity maintains information security in a manner commensurate with the size and extent of threats to its information assets, and which	There are no specific governance obligations relating to the GLBA, HIPAA or the TSA Directives.	**Financial sector** OSFI's Technology and Cyber Risk Management Guideline provides that senior management is accountable for directing the institution's technology and cyber security operations and should assign clear responsibility for technology and cyber risk governance to senior officers. Directors or officers may also be held personally liable under certain provincial privacy legislation.[106]	• See row 3(a) above. The EU Directives and Regulations that describe 'organisational' or 'risk management' measures require appropriate governance to be put in place and documented in order demonstrate compliance.	**General** For UK GDPR, UK NIS and FCA Guide see row 3(a) above. **Financial sector** The FCA has also issued guidance FCG 2.2.1G that outlines a clear expectation of senior management to take clear responsibility for managing financial crime risks, including data security.[109] The Senior Managers and Certification Regime applies to various firms in the

[91] Proposal For a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (***'AI Act'***).

[105] eIDAS art 7(e); adopted in the UK through the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019.

[106] *See, e.g.*, Québec's *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1, s. 93; Manitoba's *The Personal Health Information Act*, CCSM c P33.5, s. 64(2).

[109] FCA Guide FCG 5, FCG 2.2.1.

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
		enables the continued sound operation of the entity, • a regulated entity must clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals with responsibility for decision-making, approval, oversight, operations and other information security functions. **Telecommunications** There are no specific governance obligations relating to the *Telecommunications (Carriage Service Provider—Security Information) Determination 2022*.		**Telecommunications** As with the CCSPA, under Bill C-26's proposed amendments to the *Telecommunications Act*, any director or officer who directed, authorized, assented to, acquiesced in or participated in the commission of a violation or offence can be held liable (even if the telecommunications provider is not prosecuted for or convicted of the violation or offence). Regulators will have the power to issue administrative monetary penalties of up to CAD $25,000-CAD $50,000 per day for individuals (such as directors and officers) and CAD $10-$15 million per day in any other case.[107] Directors and officers may also be fined or imprisoned if they are convicted of committing an offence under the Act.[108]		financial sector including banks, dual-regulated insurers and solo-regulated firms regulated by the FCA only. Individuals who perform the 'Chief Operations' senior management function (for those firms who are required to appoint such an individual to this function) are required to have responsibility for managing the internal operations or technology of the firm, which would include responsibility for cyber-security. Senior managers have a statutory duty to take reasonable steps to prevent regulatory breaches in the areas for which they are accountable[110] and must fit within a broader framework of responsibilities with which the firm must comply. **Payment Services** Officers of body corporates are liable for offences if an offence under the Payment Services Regulations is shown to have been committed with the consent or connivance of the officer or attributable to any neglect on their part. It is an offence to knowingly or recklessly give information which is false or misleading in any material particular to the FCA or the Payment Systems Regulator or to any other person knowing that the information is to be used for the purpose of providing information to the FCA or the Payment Systems Regulator in connection with their functions under the Payment Services Regulations[111] – this could extend to liability for false or misleading notifications in connection with security incidents. **Telecommunications** Under the TSA Regs, a network or service provider must ensure appropriate and proportionate management of persons given responsibility for the taking of security measures on behalf of the provider, including by giving a person or committee at board level or equivalent responsibility for supervising the implementation of the security policy and ensuring effective management of persons responsible for taking security measures.[112] Regular risk reviews are

[107] Bill C-26, an Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, Part 1, s 7, Parliament of Canada.

[108] Bill C-26, an Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, Part 1, s 11(2), Parliament of Canada.

[110] FCA Handbook, Code of conduct, 2.2, Senior manager conduct rules (***COCON2.2***).

[111] Payment Services Regulations 2017, s.142.

[112] TSA Regs, reg.10(f).

#		REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
							also required at least once in any period of 12 months.[113] Appropriate and proportionate measures must be taken as are appropriate and proportionate to ensure that persons given responsibility for security measures on behalf of the provider are competent to discharge that responsibility and are given resources to enable them to do so.[114]
4	(a)	**Reporting and notification obligations attaching to cyber security incidents**	**Privacy Act** Under the Privacy Act, if an 'eligible data breach' occurs in respect of an entity, the entity must notify the OAIC and affected individuals as soon as practicable. The assessment of what is an eligible data breach should be completed as soon as practicable and generally within 30 days. **SOCI Act** Under the SOCI Act, responsible entities must notify regulators of the occurrence of a: • critical cyber security incident within 12 hours, and • other cyber security incident within 72 hours. An incident is a 'critical cyber security incident' if the incident has had or is having a significant impact (whether direct or indirect) on the availability of the asset.[115] **Telecommunications (Carriage Service Provider—Security Information) Determination 2022** The SOCI Act notifications above were reproduced and applied to carriers and	**CIRCIA** As above, under CIRCIA covered entities must report: • a covered cyber incident to CISA within 72 hours after they have a reasonable belief the incident has occurred, and • a ransomware payment as a result of an attack against the covered entity within 24 hours of payment. However, at this stage, the scope of covered entities and the types of reportable incidents have not yet been defined. CIRCIA will not take effect until the CISA publishes a Final Rule establishing these definitions. **HIPAA** Under HIPAA, regulated entities must:[118] • notify individuals affected by a data breach within 60 days, • notify prominent media outlets serving the state or jurisdiction within 60 days if the breach comprises data of more than 500 individuals of a State or jurisdiction, and	**PIPEDA** Under PIPEDA, organisations are required to: • as soon as feasible, report to the Office of the Privacy Commissioner of Canada any breach of security safeguards involving personal information that poses a real risk of significant harm to individuals,[119] • notify affected individuals about such breach,[120] • notify any other organization or government institution of such breach if it is believed such organization or institution may be able to reduce the risk of harm that could result from the breach or mitigate that harm,[121] and • keep records of all breaches[122] A breach of security safeguards is defined as the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards, or	**GDPR** Under Article 33 of the GDPR, data controllers must report personal data breaches to the relevant national data protection authority without undue delay and within 72 hours of becoming aware.[124] Controllers must also notify the data subject (without undue delay) if a personal data breach occurs that is likely to result in a high risk to the rights and freedoms of the data subject.[125] Data processors must notify data controllers of security breaches affecting personal data.[126] **NIS** Operators of essential services will be required to notify, 'without undue delay', the national computer security incident response team (or, where relevant, the competent authority) of any incident having a 'significant impact' on the provision of their services.[127] In order to determine the significance of the impact of an incident, the following parameters will be taken into account: • the number of users affected by the disruption, • the duration of the incident, and	**UK GDPR** Under the UK GDPR, controllers must notify the Commissioner within 72 hours of personal data breaches that are likely to result in a risk to the rights and freedoms of individuals.[132] Controllers must also notify the data subject (without undue delay) if a personal data breach occurs that is likely to result in a high risk to the rights and freedoms of the data subject.[133] Data processors must notify data controllers of security breaches affecting personal data.[134] **UK NIS** An OES must notify the designated authority about any incident which has a significant impact on the continuity of the essential service which that OES provides. In order to determine the significance of the impact of an incident, the following parameters will be taken into account: • the number of users affected by the disruption, • the duration of the incident, and • the geographical spread of the incident.

[113] TSA Regs, reg.11.
[114] TSA Regs, reg. 13.
[115] SOCI Act s 30BC(1).
[118] US Department of Health and Human Services Office for Civil Rights, HIPAA Administrative Simplification, Regulation Text 45 CFR 164 ss 164.404-408.
[119] PIPEDA, s 10.1(1)-(2), (7)-(8).
[120] PIPEDA, s 10.1(3)-(8).
[121] PIPEDA, s 10.2.
[122] PIPEDA, s 10.3(1).
[124] GDPR art 33(1)),.
[125] GDPR art.34.
[126] GDPR art 33(2)).
[127] NIS art 14(3)
[132] UK GDPR art. 33(1); DPA s 67(1), s 67(2).
[133] UK GDPR art.34; DPA s 68(1).
[134] GDPR art 33(2)).

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
		carriage service providers under this determination. Accordingly, they must notify the Australian Signals Directorate of the occurrence of a: • critical cyber security incident within 12 hours, and • other cyber security incident within 72 hours. **CPS 234** Under CPS 234, regulated entities must notify APRA of material cyber security incidents within 72 hours. **AFS Licence** AFS licensees must submit notifications about 'reportable situations' to ASIC within 30 days.[116] It is possible that a cyber security breach would be reportable if it is a breach or likely breach of a core obligation that is significant or an investigation into such a breach or likely breach that lasts more than 30 days.[117] Core obligations of AFS licensees are set out at section 912D(3) of the *Corporations Act* and include: • do all things necessary to ensure that the financial services are provided efficiently, honestly, and fairly • be competent to provide financial services, and • have adequate risk management systems. ASIC has also taken a policy position that: • if a cyber security risk poses a material risk to an organisation, it should consider disclosure of that risk in its annual operating and financial review, and • whether or not a cyber attack or cyber event has occurred, where it could cause a direct or indirect financial impact to an organisation, disclosure in your	• notify the Secretary of Health and Human Services within 60 days. **TSA Security Directives** The TSA Security Directives require owners and operators of regulated entities to report cyber security incidents to the CISA as soon as practicable, but no later than 24 hours after a cyber security incident is identified. Owners and operators who were not previously required to develop and adopt a Cyber security Incident Response Plan must complete their plan within 180-days of the effective date of the Security Directive. The completed vulnerability assessment form and remediation plan required by the Security Directive must be submitted to TSA within 90 days of the effective date of the Security Directive. Owners must provide in writing to the TSA within seven days of the Security Directive's effective date a notice of the commencement of new operations or change in any of the information required by the Security Directive.	from a failure to establish those safeguards.[123] If enacted, the CPPA is expected to largely maintain these existing notification requirements. Similar requirements apply under "substantially similar" provincial legislation in Québec, British Columbia, and Alberta, and reporting and notification obligations also exist under certain industry-specific provincial legislation. **Critical Infrastructure** If enacted, the CCSPA will require designated operators to immediately report any "cyber security incident" to the CSE and, immediately thereafter, to the operator's federal regulator. A cyber security incident is defined to include any act, omission or circumstance that interferes or may interfere with (i) the continuity or security of a vital service or vital system or (ii) the confidentiality, integrity, or availability of a critical cyber system. **Financial Services** OSFI's Technology and Cyber Security Incident Reporting Advisory requires that certain technology or cyber security incidents be reported by federally-regulated financial institutions to OSFI within 24 hours, or sooner if possible. Incidents are reportable if they meet any one of a range of characteristics, including for example having an impact on the institution's operations, infrastructure, data and/or systems, including but not limited to the confidentiality, integrity or availability of customer information, or having an impact that has potential consequences for other financial institutions or the Canadian financial system. IIROC's Cyber security Incident Reporting Requirements require dealer members to report to IIROC within three days of discovering a cyber security incident that	• the geographical spread of the incident. Where appropriate, the competent authority or CSIRT may inform the public about individual incidents, where public awareness is necessary to prevent an incident or to deal with an ongoing incident. **NIS 2** NIS 2 requires essential and important entities to notify, 'without undue delay', the CSIRT or competent authority of any incident having a 'significant impact' on in-scope services. These are incidents that have: • caused, or are capable of causing, severe operational disruption of the services, or • affected, or are capable of affecting, other natural or legal persons by causing considerable material or non-material damage. Under Article 23 of NIS 2, there is a tiered approach to incident reporting: [128] • submit an early warning to CSIRT within 24 hours of becoming aware of an incident, • submit an incident notification to CSIRT within 72 hours of becoming aware of an incident, • produce an intermediate report to CSIRT on request, and • produce a final report within one month of incident notification Where appropriate, entities must also communicate without undue delay to the recipients of their services, notifying them of the incident and informing them of any measures or remedies which recipients are able to take in response to that threat. As under NIS, the competent authority or CSIRT may also decide to inform the public about individual incidents, where public awareness is	The notification must be provided without undue delay and in any event no later than 72 hours after the operator is aware that an incident has occurred.[135] Where appropriate, the competent authority or CSIRT may inform the public about individual incidents, where public awareness is necessary to handle the incident or to prevent a future incident. **FSMA** The *Financial Services and Markets Act 2000 (UK)* **(FSMA)** also contains a general duty on listed companies to disclose all such information as investors would reasonably require for the purpose of making an informed assessment of the assets and liabilities, financial position, profits and losses, and prospects of the company.[136] **Other regulations** Under the *Communications Act 2003*, public electronic communications providers must: • take reasonable steps to bring a security compromise to the attention of persons who use the network or service,[137] and • Inform Ofcom (**Office of Communications**) about a significant security compromise.[138] The Telecommunications Security Code of Practice provides guidance on complying with the *Communications Act 2003* and the amendments in the *Telecommunications (Security) Act 2021*. Please see row 3(a) for other notification obligations for sector-specific legislation.

[116] ASIC, 'Reportable situations for AFS and credit licensees'.
[117] ASIC, 'Regulatory Guide RG 78 Breach reporting by AFS licensees and credit licensees'.
[123] PIPEDA, s 2(1).
[128] NIS 2 art 23(4)
[135] UK NIS s 11(1), s 11(3)(b)(i).
[136] *Financial Services and Markets Act 2000 (UK)* s 80 (***Financial Services and Markets Act***).
[137] *Communications Act 2003*, as amended by *Telecommunications (Security) Act 2021* s 105K (***Communications Act***).
[138] Communications Act s 105K.

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
		annual financial report may be appropriate to avoid the risk of a material misstatement.		is reasonably likely to result in (i) substantial harm to any person and/or material disruption to operations, (ii) invoking the firm's business continuity or disaster recovery plan, or (iii) reporting obligations under any applicable laws to a government body or regulatory authority or organization. IIROC also requires that, within 30 days of discovering such an incident, the dealer member report details regarding its investigation of the incident.	necessary to prevent an incident or to deal with an ongoing incident. Additionally, the Commission Regulation[129] clarifies how PECS providers should meet their notification obligations under the e-Privacy Directive.[130] This include informing the relevant national data protection authority of the incident within 24 hours after detection of the breach.[131] Also note notification obligations under sector-specific legislation (e.g. PSD2, the Electronic Identification Regulation, EECC and the e-Privacy Directive) set out in the row above. **EU Artificial Intelligence Regulation (AI Act)** Under the proposed AI Act, providers of 'high risk' AI systems would have obligations to inform national competent authorities about serious incidents or malfunctions that constitute a breach of fundamental rights, as well as any recalls or withdrawals of AI systems from the market.	
(b)	**Governance Implications**	The notification requirements are complex due to the fact that an organisation may have to notify multiple regulators of the same cyber incident. This is compounded by the fact that if listed, the organisation may well have to notify the exchange at the same time, given that any cyber incident that is reported is likely to be price sensitive. Governance arrangements will need to be put into place to ensure that these notifications will be able to be approved and made in a timely manner. More generally, boards must ensure that their risk management frameworks are sufficient to identify and manage cyber risks. Failure to do so could result in the directors breaching their fiduciary duty, including the duty to act with due skill and diligence. This means that directors should satisfy themselves that: • cyber risks are adequately addressed by their risk management frameworks, and that controls are implemented to	The analysis for Australia applies equally in the US.	In addition to the above-discussed governance implications associated with OSFI and the proposed CCSPA, the notification requirements across federal and provincial statutes can be complex due to the fact that an organisation may have to notify multiple regulators of the same cyber incident. Governance arrangements will need to be put into place to ensure that these notifications will be able to be approved and made in a timely manner. Separately, the analysis for Australia in relation to directors' duties also applies in Canada.	The notification regimes are complex in the EU due to requirements to notify individuals or data subjects in addition to regulators. This has created a step change in how boards need to address cyber security incidents and manage reputational risk. This is compounded by: • multiple regulatory regimes requiring potentially numerous regulatory notifications; and • the close nature of processing in Member States of the EU, requiring consideration of notifications in multiple jurisdictions. In particular, notification should be made to the lead supervisory authority in the event of a personal data breach relating to cross-border processing within the EU. Where there is no lead supervisory authority, then consideration will need to be given as to which supervisory authorities should be notified.	The same considerations for governance generally apply in the UK as they do in the EU, save that there is no recognition of a lead supervisory authority for personal data breaches impacting on the UK and also on Member States in the EU. The ICO should be notified of personal data breaches that are subject to the UK GDPR and DPA. Additionally, the analysis for Australia in relation to directors duties also applies in the UK. Particular consideration should be given to sector-specific rules implementing additional governance requirements impacting on the board (e.g. in respect of Telecoms Security) or in which directors or senior managers could have liability (e.g. Financial sector under the SM&CR regime or Payment services in respect of false or misleading notifications to the regulator) (see row 3 above). Consideration needs to be given to which regulator is likely to take the lead in respect of cyber security incidents; for example where a sector-specific

[129] (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications (***Commission Regulation***).

[130] Commission Regulation.

[131] Commission Regulation art 2(2), (3).

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
		protect key assets and enhance cyber resilience, • their organisations are cyber resilient, are able to manage disruptions caused by cyber security incidents, and to detect, manage and recover from incidents. The risk management plans for cyber incidents will need to ensure that there are appropriate processes and procedures in place to: • convene the organisation's crisis management team to respond to and manage a cyber incident and implement the organisation's cyber response plans, • notify the board and keep it informed of progress on the response and impact of the cyber incident on the organisation, its customers and other stakeholders, and • notify appropriate regulators, customers and the market if the cyber incident meets the requisite thresholds for those notifications.			This is compounded by the fact that if listed, the organisation may well have to notify the exchange at the same time, given that any cyber incident that is reported is likely to be price sensitive. Governance arrangements will need to be put into place to ensure that these notifications will be able to be approved and made in a timely manner. Separately, the analysis for Australia in relation to directors duties also applies in the EU. There are no specific obligations on company directors, but natural persons can be held liable for breaches of reporting obligations under the GDPR (see row 1) and NIS 2 (see row 2).	regulator like the FCA or Ofcom may be involved in respect of an incident. Plans should be made as to which regulator is likely to take the lead and who may take priority for particular incidents.
5	(a) **Listed company disclosure obligations relating to cyber security incidents**	ASX Listing Rule 3.1 requires a company to immediately disclose information that a reasonable person would expect to have a material effect on the price or value of its securities. "Immediately" means "promptly and without delay". In practice, ASX recognises the speed of disclosure may vary depending on the circumstances, including having regard to: • the forewarning (if any) the entity had, • the amount and complexity of the information concerned, • the need (in some cases) to verify the accuracy of information,	The SEC's *Guidance on Public Company Cyber security Disclosures* notes that public companies are expected to inform investors about material cyber security risks and incidents in a timely fashion.[141] Public companies further have a duty to update and correct prior disclosures, such as if the company later learns of a large cyber security attack after the disclosure was made. Additionally, in March 2022, the SEC issued proposed amendments to its rules to enhance and standardise disclosures regarding cyber security incident reporting by public companies.[142] Amongst other things, the proposed amendments would: • require registrants to disclose information about a material	The Canadian Securities Administrators is an umbrella organization for Canada's provincial and territorial securities regulators. The CSA's *Multilateral Staff Notice 51-347 Disclosure of Cyber Security Risks and Incidents* requires reporting issuers to disclose cyber security incidents where such incidents result in a material fact or material change that requires disclosure in accordance with general securities legislation. An assessment of materiality requires a contextual analysis: there is no bright-line test and the quantitative or qualitative threshold at which a cyber security breach becomes material may vary between issuers and industries, depending on the circumstances of the	Publicly listed companies are required to inform the public as soon as possible of inside information which directly concerns that issuer and could affect the price of securities.[143] 'Inside information' may include the occurrence of a cyber security breach. Listing rules and guidance in Member States may also prescribe additional reporting obligations for listed companies.	The EU MAR applies in the UK under the *European Union (Withdrawal) Act 2018 (UK)*[144]. It requires publicly listed companies (or 'issuers') to inform the public as soon as possible of inside information which directly concerns that issuer.[145] 'Inside information' may include the occurrence of a cyber security breach. A listed company whose equity shares are admitted to trading on a regulated market should comply with this requirement.[146]As stated above, the *Financial Services and Markets Act 2000 (UK)* also contains a general duty on listed companies to disclose all such information as investors would reasonably require for the purpose of making an informed assessment of the assets and liabilities, financial position,

[141] Securities and Exchange Commission, 'Commission Statement and Guidance on Public Company Cyber security Disclosures'.

[142] Securities and Exchange Commission, 'Cyber security Risk Management, Strategy, Governance and Incident Disclosure'.

[143] Regulation (EU) No 596/2014 (***EU MAR***), art. 17.

[144] *European Union (Withdrawal) Act 2018 (UK)* (***Withdrawal Act***).

[145] EU MAR art 17(1).

[146] FCA Handbook, Listing Rules, 9.2.5.

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
		• the need for an announcement to be accurate, complete and not misleading, and • the need (in some cases) for approval by the entity's board or disclosure committee. When assessing whether an entity is in compliance with their continuous disclosure obligations, ASX recognises that the sensitivity of the market to information is at its highest during trading hours. This, in effect, means that ASX expects more prompt disclosure when the entity is trading vs when they are not (such as when they are in a trading halt). While Listing Rule 3.1 is subject to a number of exceptions, the exceptions all require that the information in question remains confidential. Given confidentiality cannot be assured in the context of a cyber security incident, it may be difficult for an entity to rely on any exception to continuous disclosure in relation to the incident. This is particularly so given both ASIC and the ASX take the view that for listed companies significant cyber incidents are likely to be material events that should be disclosed[139]. There is obviously a complex decision to be made around disclosure of an incident in circumstances where information about the incident is evolving or unclear. The ASX has indicated that it's reasonable if the company is not already aware of the market-sensitive information for it to seek a brief trading halt / voluntary suspension, while they "conduct the investigations they need to get the facts they can disclose to the market".[140] To minimise any risks associated with continuous disclosure obligations and to assist in ensuring that there is not a false market in securities, a company and its directors should: • take steps to ensure that any disclosures to the market are accurate and not misleading, including by omission. Any	cyber security incident within four business days after the entity determines that it has experienced a material cyber security incident; • require registrants to provide updated disclosure relating to previously disclosed cyber security incidents; • require disclosure when a series of previously undisclosed individually immaterial cyber security incidents has become material in the aggregate; • require foreign private issuers to report on cyber security incidents; and • require annual reporting or certain proxy disclosures about the board of directors' cyber security expertise and oversight role for cyber security risks. The proposed amendments are currently undergoing regulatory review.	issuer as well as on the type of incident and the extent of the consequences. The CSA's Multilateral Staff Notice notes that the timing of a disclosure is an important consideration but acknowledges that cyber security incidents may not be detected until much later than when they occurred, and the consequences of the incident may take time to fully assess. The Notice recognizes that the determination of whether an incident is material is a dynamic process throughout the detection, assessment and remediation phases of the incident. Canadian securities regulators expect issuers to address in any cyber attack remediation plan how materiality of an attack would be assessed to determine whether and what, as well as when and how, to disclose in the event of an attack. Where an issuer has determined a cyber security incident should be disclosed, it might also be appropriate to consider and provide visibility as to the anticipated impact and costs of the incident.		profits and losses, and prospects of the company, in its listing particulars.[147] Additional continuing disclosure obligations may apply depending on the nature of a company's listing. For example, the AIM Rules require AIM-listed companies to issue notification without delay of new developments which are not public knowledge which, if made public, would be likely to lead to a significant movement in the price of its AIM securities.[148]

[139] See https://www.afr.com/technology/only-11-of-36-hacks-revealed-to-market-asic-warns-on-disclosure-20230216-p5cl28

[140] Paul Smith, 'Disclosure questions emerge as ASX braces for wave of cyber halts', Australian Financial Review, (8 November 2022).

[147] *Financial Services and Markets Act 2000 (UK)* s 80 (***Financial Services and Markets Act***).

[148] AIM Rules for Companies, rule 11.

#		REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
			statements made must also have a reasonable basis; and • ensure that it is as well prepared as possible to manage disclosure of any further price sensitive information.				
	(b)	**Governance Implications**	Cyber security risk is a risk (like many other risks) that a company faces. As stated above, from a governance perspective, boards have responsibility for oversight of appropriate risk management frameworks that sufficiently identify and manage a company's cyber risks. Failure to do so could result in the directors breaching their duty to act with due skill and diligence under section 180 of the *Corporations Act 2001* (Cth). Directors should also note the requirements of CPS 234 in row 3 above.	In order to fulfil fiduciary duties owed to shareholders (including duties of care and loyalty), directors and officers of public companies must ensure they exercise appropriate governance over cyber security risk, including by being properly informed about the relevant risks and the steps taken by the company to address such risks.[149] Boards will also need to ensure that investment risks are accurately disclosed to investors. Boards and officers have faced scrutiny and litigation relating to their oversight of the company's security. For example, in relation to the Yahoo! data breaches, shareholders brought a derivative action against individual board members and officers, alleging that they had failed to: • properly disclose the security incidents, • ensure that proper security measures were in place, and • investigate the relevant incident. A claim was further brought against Verizon (who had purchased Yahoo!'s operating assets) for aiding and abetting the alleged fiduciary breaches. The insurance carriers have agreed to pay US $29 million in a settlement.[150] The SEC issued an US $35 million fine in relation to the same incident.[151]	Under Canadian law, directors and officers of a corporation are required, in exercising their powers and discharging their duties, to exercise the care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances.[152] This duty of care, diligence and skill is likely to extend to matters of cyber security. A failure to ensure that an organisation adequately addresses cyber security risks, or failures to adequately and truthfully represent an organisation's cyber security posture, measures, incidents or risks, could expose directors to personal liability.	Boards of listed companies must ensure that their risk management frameworks are sufficient to identify and manage cyber risks and to ensure that it has systems in place to manage disclosures required to be made to the market.	The UK Corporate Governance Code (**CGC**) applies to publicly listed companies and contains provisions that are relevant to the management of cyber security risks. Clause 28 for instance, requires boards to carry out a robust assessment of the company's emerging and principal risks. This clause also states that in its annual report, a board should: • confirm that it has completed an assessment • describe the principal risks • describe the procedures in place to identify emerging risks, and • explain how these emerging risks are being managed or mitigated.[153] The GCG also states that the board should monitor the company's risk management and internal control systems, and assess them annually.
6	(a)	**Presence of direct rights of action or statutory tort arising out of a cyber security or data breach**	There are currently no direct rights of action or statutory torts arising out of these matters in Australia. In particular, the *Privacy Act* does not allow for a private right of action to individuals if an entity subject to that Act breaches the APPs in that Act or otherwise commits an interference with privacy. There is	At present, there is no statutory tort arising out of a cyber security or data breach. More broadly, there is no private right of action under federal legislation. However, certain state legislation (e.g.	Under PIPEDA, individuals do not have a direct and immediate right of action for violations of the Act. An individual must first make a formal complaint to the OPC alleging an organisation's failure to comply with its obligations to collect, use or disclose personal information in accordance with PIPEDA, including the	The GDPR provides data subjects with the right to: • Receive compensation from data controllers or processors if they suffer material or non-material damage as a result of an infringement of the GDPR,[156]	The UK GDPR gives data subjects the right to: • Receive compensation from data controllers or processors if they suffer material or non-material

[149] See *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).
[150] Notice of Pendency and Proposed Settlement of Shareholder and Derivative Actions at ¶ 35.
[151] Administrative Proceeding File No. 3-18448 (SEC Order against Yahoo!).
[152] *Canada Business Corporations Act 1985* (Can) s 122(1).
[153] Financial Reporting Council, UK Corporate Governance Code (2018), clause 28 (***GCG***).
[156] GDPR art 82.

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
		provision for a representative claim to be made to the OAIC but determinations by the OAIC are not binding and have to be enforced de novo in a court of law. Australian law does not include a statutory tort for invasions of privacy. However, as noted above, the Privacy Act Review Report has recently proposed the introduction of both a private right of action, as well as a statutory tort.	the *California Consumer Privacy Act*) creates a data breach right of action.	Fair Information Principles.[154] After receiving the OPC's report or being notified that the investigation of the complaint has been discontinued, the complainant may apply to the Federal Court for an order that the organization correct its practices, an order requiring the organization to publish a notice of any action taken or proposed to be taken to correct its practices, or damages, including damages for any humiliation suffered. The proposed CPPA would create a new private right of action that gives a cause of action for damages to any individuals affected by an act or omission that contravenes the CPPA.[155] Such an action can be brought in Federal Court or in a provincial superior court, but only after the Privacy Commissioner or the proposed Personal Information and Data Protection Tribunal finds that the organization has contravened the CPPA or after the organization is convicted of an offence under the CPPA. Certain provinces, including British Columbia, have created statutory torts for violations of privacy that do not require proof of damages.	• Lodge a complaint with the Commissioner for an infringement of the GDPR, [157] and • Be informed by the Commissioner about any available judicial remedies.[158] Specific processes will vary by EU member state. Other causes of action may also exist, for example between controllers and processors, but also in the case of data subjects arising out of national implementations of the e-Privacy framework and based on other common or civil law principles. See row 7(a) below for actions brought by consumer representative bodies.	damage as a result of an infringement of the UK GDPR,[159] • Lodge a complaint with the Commissioner for an infringement of the UK GDPR, [160] and • Be informed by the Commissioner about any available judicial remedies.[161] See row 7(a) below for actions brought by consumer representative bodies. The DPA provides that persons suffering damage (comprising financial loss as well as damage not involving financial loss such as distress) due to a contravention of the UK GDPR or other data protection legislation are entitled to compensation from the relevant controller or processor.[162] Claims from data subjects often also invoke the PECR regime[163] (the UK's implementation of the e-Privacy Directive[164]; as well as the (non-statutory) torts of misuse of private information and, less commonly now in this sphere, breach of confidence.
(b)	**Governance implications**	There are currently no governance implications as there is no statutory tort or private right of action available. However, should a private right of action or statutory tort in relation to interferences or invasions with privacy become available, this does increase the risk to organisations of class actions. Class actions have major implications for director risk and liability, with increasing numbers of class actions against directors taking place in other jurisdictions. In this context it becomes more important to ensure that directors are able to make informed decisions on behalf of their companies without the fear of being held personally liable. The	There are no governance implications as there is no statutory tort or private right of action available.	It is currently unclear whether organizations will be exposed to class actions under the CPPA, including given that, under the proposed legislation, any individual "affected" by the CPPA contravention would have a right of action, as opposed to just the complainant, as is currently the case under PIPEDA. Should class actions be available, this could have major implications for director risk and liability. In this context it becomes more important to ensure that directors are able to make informed decisions on behalf of their companies without the	There is no explicit cause of action against company directors under the GDPR, however, data subjects may be able to claim compensation from directors given that 'natural persons' can be liable for breaches of the GDPR.	There is no explicit cause of action against company directors under the UK GDPR, however, data subjects may be able to claim compensation from directors given that 'natural persons' may be liable for breaches of the UK GDPR. Please see our further commentary regarding liability of directors in row 1 above.

[154] Ling et al, 'Cyber security Laws and Regulations Canada 2023' in in *Cyber security Laws and Regulations* (ICLG, 14 November 2022).
[155] Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts, s. 107, Parliament of Canada.
[157] GPDR art 77 (1).
[158] GPDR art 77 (2).
[159] UK GDPR art 82; DPA s 168.
[160] UK GPDR art 77 (1).
[161] UK GPDR art 77 (2).
[162] UK Data Protection Act 2018 sections 168 and 169.
[163] Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended): including by virtue of section 30.
[164] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

#		REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
			availability of Directors and Officers Insurance plays a critical role in assisting them to do so.[165]		fear of being held personally liable. The availability of Directors and Officers Insurance plays a critical role in assisting them to do so.		
7	(a)	**Class action settings**	There is currently limited scope for class actions relating to cyber breaches. As above, this is because there is no direct right of action or statutory tort arising out of a cyber security or data breach. However, in February 2023, a class action was initiated against Medibank in respect of its 2022 data breach, alleging breach of contract, contraventions of the Australian Consumer Law and breach of confidence. As noted above, there is provision for representative claims to be made to the OAIC but determinations by the OAIC are not binding and have to be enforced de novo in a court of law. However, the Privacy Act Review Report, which was published in February 2023,[166] proposes the introduction of a direct right of action to enable individuals to apply to the courts for relief in relation to privacy breaches, as well as the introduction of a statutory tort for serious invasions of privacy. The combined effect of these proposals could result in increased levels of litigation on privacy matters, including through representative groups.	Class actions for cyber security breaches have become increasingly common although no direct right of action or statutory tort exists. Generally, actions have been brought on grounds including breaches of express or implied contracts, negligence, other common law torts, or breaches of consumer protection legislation.[167] To establish standing, plaintiffs must show that they suffered an injury-in-fact, though this may nevertheless be insufficient for a claim of damages.[168] A class action lawsuit was also brought against Yahoo! for the data breaches set out above. The final settlement fund totalled US $117.5 million.[169] There has also been an increase in shareholder derivative actions (see the example relating to the Yahoo! data breaches set out above).	Class actions regarding cyber security breaches are occasionally brought, although, as discussed above, there is no federal direct right of action (with the exception of a claim by a complainant under PIPEDA) or statutory privacy tort. Class action claims are therefore often grounded in provincial statutory torts and common law torts (such as negligence) and/or breach of contract. Subject to claims pursuant to provincial statutory torts that do not require proof of damages, Canadian courts have been broadly sceptical of data breach claims, often dismissing or refusing to certify class actions due to a lack of evidence that class members suffered compensable harm or that any harm suffered was in fact caused by the cyber security breach.[170] Several Canadian courts have also recently rejected the application of the tort of intrusion upon seclusion against defendants who collect personal information and thereafter suffer cyber security breaches (*i.e.*, "database defendants"), on the view that such defendants had not themselves committed the "intrusion". No class actions involving director or officer liability for cyber security incidents have to date been decided. It is worth noting that, as of September 2023, Québec's private-sector privacy law will provide for punitive damages of at least CAD $1,000 for unlawful infringements of privacy rights that cause injury and are intentional or result from a gross fault. The availability of such	As data subjects have a direct right of action in the EU, there is good scope for class actions related to cyber security and data breaches. Data subjects can mandate a not-for-profit body, organisation or association to bring data protection representative action in the EU (subject to national laws).[171] Even more, the CJEU has recently ruled that consumer protection associations can raise class-action type lawsuits on behalf of individuals without first obtaining their consent to do so, so long as there is a link between data processing practices and alleged non-compliance with consumer protection laws.[172] In particular, the CJEU has noted that in order for consumer protection associations to bring the representative action, they do not need to: • carry out a prior individual identification of the relevant individual, or • specify the existence of a specific infringement. Rather, it is open to consumer protection associations to simply: • refer to individuals they wish to represent by indirect identifiers (e.g. location data), and • 'consider' that data subjects' rights have been infringed by virtue of the way the data has been processed.	Courts in England and Wales have not traditionally entertained class actions in the opt-out American sense of the word. Nonetheless, there have been attempts, driven by claimant firms and funders, to bring about this culture. Where multiple claims arise in relation to a single set of facts, such as a data breach, there are various ways in which they can be consolidated as a group (or "class") action, although typically in England these are opt-in proceedings rather than opt-out. In addition to the courts' general discretion to consolidate proceedings for case management purposes, the Civil Procedure Rules provide for both Group Litigation Orders and Representative Claims to be litigated. The decision of the UK Supreme Court in *Lloyd v Google,*[173] did not allow a representative (opt-out) claim for a cyber security breach under section 13 of the *Data Protection Act 1998 (UK)*. The Supreme Court determined that compensation could not be awarded under the DPA for 'loss of control' without material evidence of damage or distress, but they did not rule out of the use of opt-out representative actions under the DPA and UK GDPR.[174] In fact, while noting the various shortfalls of a representative proceedings in a case relating to data security, the Court still seemed to encourage the use of this type of proceeding in appropriate cases.[175] Nonetheless, this decision is commonly held to have dampened the enthusiasm of litigation funders and claimant firms for US style opt-out class actions, with the focus perhaps shifting to related

[165] https://www.apra.gov.au/class-action-and-growing-importance-of-directors-and-officers-insurance
[166] Attorney-General's Department, 'Privacy Act Review Report', (2022) (***Privacy Review Report***).
[167] Edward McNicholas and Kevin Angle, 'Cyber security Laws and Regulations USA' in *Cyber security Laws and Regulations* (ICLG, 14 November 2022) 6.1.
[168] Edward McNicholas and Kevin Angle, 'Cyber security Laws and Regulations USA' in *Cyber security Laws and Regulations* (ICLG, 14 November 2022) 6.1.
[169] See Second Amended Order Granting Plaintiffs' Motion for Final Approval of Class Action Settlement at 19.
[170] Gelowitz et al, 'Canadian Courts Confirm Significant Limits on Privacy Class Actions', *Canadian Privacy Law Review* (2022)
[171] GDPR art 80.
[172] GDPR art 80; Pinsent Masons, 'EU law on representative data protection class actions clarified' (2 May 2022); see in particular GDPR art 80.
[173] [2021] UKSC 50 (***Lloyd***).
[174] Note, the Court did not rule that an opt-in claim could not be brought, but they warned against it, given the low participation rates in previous opt-in class actions, see *Lloyd* at [26]-[28].
[175] *Lloyd* at [84]-[89].

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
				damages is likely to incentivize additional class actions.		areas of law where these may be easier to establish, such as in competition law where it can be applied to data matters. *Lloyd v Google* did not directly address causes of action under the UK GDPR. The England and Wales High Court recently allowed a representative action to be brought against various Tik Tok entities under the UK GDPR in *SMO v TikTok Inc. and others,*[176] however, this case does not concern a cyber security breach and it is understood that the claim was withdrawn after the decision in *Lloyd* with the Children's Commissioner (representing the claimants) citing concerns about costs. UK Courts 'may have regard' to decisions of the Europeans Courts in their consideration of any retained EU Law.[177] This is important given that the CJEU has recently allowed actions from consumer groups against large data controllers under the EU GDPR.[178] Failure to comply with disclosure requirements in the *Financial Services and Markets Act* can also provide a cause of action for a collective compensation claim.[179]
	(b)	**Governance implications**	As stated above, class actions have major implications for director risk and liability, with increasing numbers of class actions against directors taking place. It is important to ensure that directors are able to make informed decisions on behalf of their companies without the fear of being held personally liable. The availability of Directors and Officers Insurance plays a critical role in assisting them to do so.[180] See also row 6(b).	See rows 6(b) and 7(a).	See rows 6(b) and 7(a).	See rows 6(b) and 7(a).	See rows 6(b) and 7(a).
8	**(a)**	**Identity of key cyber security regulator**	The Department of Home Affairs plays a very significant central and coordinating role in relation to cyber security because of its administration of the SOCI Act which covers many industry sectors. The OAIC in respect of breaches of the *Privacy Act*. APRA in respect of CPS 234.	There is no single cyber security regulator in the United States. However, some of the key federal regulators are: • the FTC, who is the principal US federal privacy regulator, and covers most for-profit businesses,	Organisations subject to PIPEDA are regulated by the Office of the Privacy Commissioner of Canada (**OPC**). Organisations operating in provinces with "substantially similar" privacy legislation, namely Québec, British Columbia, and Alberta, are regulated by the privacy commissioners of those provinces.	In the European Union, there is no overarching cyber security regulator. Member States have the ability to appoint competent supervisory authorities in areas that are regulated by EU directives and regulations. A list of EU national data protection authorities can be found here: List of EU National Data Protection Authorities	The Information Commissioner's Office is the general regulator in respect of privacy and cyber security. The ICO covers the following: • The DPA and UK GDPR, • Privacy and Electronic Communications Regulations,

[176] [2022] EWHC 489 at [95].

[177] Withdrawal Act s 6(2).

[178] *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V.* (C-319/20) [2022] CJEU.

[179] Financial Services and Markets Act s 90.

[180] https://www.apra.gov.au/class-action-and-growing-importance-of-directors-and-officers-insurance

#		REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
				• the SEC, in respect of many financial institutions and listed entities, and • CISA and the TSA, entities within the Department of Homeland Security, in respect of US critical infrastructure. The U.S. Department of Health and Human Services and Office for Civil Rights, in respect of critical cyber security related to healthcare.[181]	Federally regulated financial institutions are also regulated by OSFI and operators of critical infrastructure are regulated by industry-specific regulators or ministries.	There are however a number of EU bodies with responsibilities in connection with EU laws relating to cyber security, including the European Data Protection Board, which is established under the EU GDPR as an independent body composed of representatives of EU national data protection authorities and contributes to consistent application of the data protection rules throughout the EU and cooperation between EU national data protection authorities.	• UK NIS in respect of relevant digital services, and • UK eIDAS, Other regulators have responsibility for relevant sectors or legislation, including: • PRA/FCA – financial sector, • Ofcom – telecoms (i.e. Communications Act) and digital infrastructure (i.e. UK NIS), A range of government bodies and regulators have responsibility under UK NIS – see Schedule 1 of the UK NIS.
	(b)	**Governance implications**	Companies should make sure they know which regulator(s) are relevant to their sector and necessary to contact for each type of cyber security incident. This is important for the purposes of ensuring a company has access to the appropriate support if a breach occurs. In general, companies should aim to develop and maintain good working relationships with regulators.	N/A	The recommendation for Australia also applies in Canada.	Under the EU GDPR, organisations can select a lead supervisory authority where they carry out cross-border processing in the European Union. For businesses undertaking cross-border processing, it is critical to understand and where appropriate select a lead supervisory authority for privacy.	It is important to ensure that companies understand who the relevant regulatory bodies are for their business and their products and services in the UK. Cyber incidents could require notification with different regulators and it is generally seen as important in the UK to have a good working relationship with regulators to assist in the event that cyber incidents occur.
9	**(a)**	**Level of guidance and support the cyber security regulator provides industry**	The Department of Home Affairs has published multiple draft guidance documents on the application of the regulatory regime that applies under the *SOCI Act*.[182] The OAIC provides a significant amount of guidance and explanation relating to obligations to notify eligible data breaches.[183] APRA provides a Prudential Practice Guide to CPS 234.[184] ASIC provides guidance to regulated entities on cyber resilience and has in the past published report 429 Cyber resilience: Health check to help	The FTC issues privacy and data security guidelines that are considered "best practice".[187] The CISA also publishes guidance documents and recommendations on how entities can protect and enhance the resilience of the nation's physical and cyber infrastructure.[188] As discussed above, the TSA implements security directives regarding cyber security. The SEC has provided guidance to assist public companies in preparing disclosure about cyber security risks and incidents.[189]	The OPC regularly provides guidance on PIPEDA compliance and interpretation. OSFI has issued cyber risk management guidance for federally regulated financial institutions.[191] Additionally, CSE operates the Canadian Centre for Cyber Security, which provides expert advice, guidance, services, and support. Among other things, the Centre issues alerts and advisories on potential or imminent cyber threats and incidents.	ENISA publishes a range of guidance on best practices for cyber security.[192] ENISA provides guidance in respect of cyber security for data protection, e-Privacy, communications and electronic trust services, among other things. In addition, there is a range of general and sector-specific guidance that is issued by different supervisory and regulatory bodies in the EU, including (but not limited to): • Privacy: The EDPB provides guidance on a range of issues relating to privacy including on data breach notifications;[193] and • Financial sector: The European Banking Authority publishes	The ICO publishes a variety of guidance materials, including the Guide to the UK GDPR.[195] Other regulators with responsibility for cyber-security in relation to critical national infrastructure or particular sectors also publish guidance, some of which companies must comply with to demonstrate that they are meeting the requirements of relevant cyber security regulations. For example: • Telecoms: Telecommunications Security Code of Practice,[196] • Financial sector: Bank of England Supervisory Statement (SS2/21) on Outsourcing and third party risk management, and

[181] Who enforces the privacy and security standards established under HIPAA | HHS.gov

[182] DRAFT SOCI risk management (RMP) Rules 2022; DRAFT Protected Information Guidance Material – Industry; Approval of Responsible Entity Risk Management Program Annual Report.

[183] OAIC, 'Data breach preparation and response', (2019).

[184] APRA, 'Prudential Practice Guide', (June 2019).

[187] See, Federal Trade Commission, 'Start with Security', (Report, June 2015).

[188] See, Cyber security and Infrastructure Security Agency, 'ICS Recommended Practices'.

[189] See, Securities and Exchange Commission, 'Commission Statement and Guidance on Public Company Cyber security Disclosures' (26 February 2018).

[191] *See, e.g.*, Office of the Superintendent of Financial Institutions, 'Technology and Cyber Risk Management', (July 2022).

[192] ENISA, 'Guidelines'.

[193] See, Cyber security and data breach | European Data Protection Board (europa.eu)

[195] Information Commissioner's Office, 'Guide to the General Data Protection Regulation (GDPR)'.

[196] Department for Culture, Media and Sport, December 2022.

#		REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
			organisations improve cyber resilience[185]. While not a regulator, in October 2022, the Australian Institute of Company Directors in conjunction with the Cyber security Cooperative Research Centre published The AICD CSCRC Cyber Security Governance Principles that provide a clear and practical framework for organisations to build stronger cyber resilience.[186]	The HHS has provided cyber security guidance materials, including an OCR Cyber Awareness Newsletter.[190]		guidance on outsourcing and third party risk management.[194]	• Digital infrastructure: Guidance for the digital infrastructure subsector under the UK NIS (Ofcom, 2021). The National Cyber Security Centre (***NCSC***) also provides guidance on cyber security and operates the Cyber Essentials and Cyber Essentials Plus certification schemes for cyber security.
	(b)	**Governance implications**	See row 9(a).	See row 9(a).	See row 9(a).	See row 9(a). Most guidance in the EU on cyber security will include elements of organisational measures that should be taken into account in companies' cyber risk management frameworks. It is important to recognise which guidance applies to the business and understand if the guidance is binding or can be used as evidence of compliance or non-compliance with relevant laws and regulations in the EU.	See row 9(a). Most guidance in the UK on cyber security will include elements of organisational measures that should be taken into account in companies' cyber risk management frameworks. It is important to recognise which guidance applies to the business and understand if the guidance is binding or can be used as evidence of compliance or non-compliance with relevant laws and regulations in the UK.
10	**(a)**	**Mechanisms or frameworks to facilitate the sharing of intelligence or support in the event of a significant cyber security incident**	The Cyber and Infrastructure Security Centre has been established by the Department of Home Affairs to drive an all-hazards critical infrastructure resilience regime under the *SOCI Act*. Its functions include: • Performing regulatory functions and exercising regulatory powers under the SOCI Act, • Providing best-practice advice, exercises, modelling and regulation that uplifts the security and resilience of all 11 critical infrastructure sectors, • Bringing together stakeholders from across the critical infrastructure community to share information and approaches to resilience and security.	The *Cyber security Information Sharing Act* 2015 encourages companies to share information about cyber security threats, incidents, vulnerabilities and defensive measures through CISA's Automated Indicator Sharing (**AIS**) tools.[197] AIS enables the real time exchange of cyber threat indicators and defensive measures. Participants are offered anonymity, as well as liability and privacy protections to encourage the submission of cyber threat indicators and defensive measures. However, use of the tools is not mandatory. In addition, the recent cyber security strategy from the Biden Administration noted that CISA and Sector Risk Management Agencies will explore technical and organisational mechanisms to enhance and evolve machine-to-machine sharing of data.[198]	**Canadian Centre for Cyber Security** As discussed above, CSE is the technical authority in Canada for cyber security and information assurance. As part of its mandate, CSE operates the Canadian Centre for Cyber Security, which issues alerts and advice on potential, imminent or actual cyber threats, vulnerabilities or incidents relevant to Canada and Canadians. **Industry-Specific Information Sharing and Analysis Centers** A number of industry-specific ISACs, including the Financial Services ISAC, operate in Canada and facilitate cyber intelligence sharing among members. **Canadian Cyber Threat Exchange** The Canadian Council of Chief Executives also created **CCTX** as a platform for	NIS required member states to designate a national single point of contact and create a co-operation network between the SPOC and ENISA to co-operate on NIS risks and incidents. NIS also required member states to set up at least one computer security incident response team to handle NIS risks and incidents for each of the critical infrastructure sectors market operators were active in. Amongst other things, CSIRTs would play a role in informing affected member states where an incident notified has a significant impact on the continuity of essential services. NIS 2 further builds on this by creating a European vulnerability database that would allow organisations to voluntarily disclose and register publicly known vulnerabilities. Each member state shall designate one of its CSIRTs as a co-	UK NIS designated the Government Communications Headquarters (GCHQ) as the SPOC and the CSIRT.[201] The proposed reforms to UK NIS mention the intention to promote greater information sharing, but do not mention the UK's participation in the EU-CyCLONe.[202] The National Cyber Security Centre (**NCSC**) has been established to provide support during cyber incidents. This provides a single point of contact for organisations, government and the general public. The NCSC: • provides practical guidance on cyber security, and • responds to cyber security incidents to reduce harm caused. The NCSC also has a division focused on critical national infrastructure. These are: chemicals, civil nuclear,

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

[186] See https://www.aicd.com.au/risk-management/framework/cyber-security/cyber-security-governance-principles.html.

[190] See Cyber Security Guidance Material | HHS.gov.

[194] See, EBA Guidelines on ICT and security risk management (2019); EBA Guidelines on security measures for operational and security risks under PSD2 (2017); EBA Guidelines on outsourcing arrangements (2019).

[197] *Cyber security Information Sharing Act 2015* s 105.

[198] *National Cyber security Strategy* (Report, March 2023) 10.

[201] UK NIS s 4.

[202] UK Department of Digital, Culture, Media & Sport, 'Proposal for legislation to improve the UK's cyber resilience', (30 November 2022).

#		REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
			The Australian Cyber Security Centre has been established to lead the Australian Government's efforts to improve cyber security. Its functions include: • providing cyber security advice and assistance to individuals, businesses and critical infrastructure operators in the event of a cyber security incident, • working with business, government and academic partners and experts in Australia and overseas to investigate and develop solutions to cyber security threats, • operating a national footprint of Joint Cyber Security Centres where it collaborates with business, government and academic partners on current cyber security issues, • working with law enforcement authorities to fight cybercrime. AusCERT (operated under the Joint Cyber Security Centres as part of the ACSC) facilitates cyber security threat information sharing and monitoring.	The government will also 'increase the speed and scale of cyber threat intelligence sharing to proactively warn cyber defenders and notify victims when the government has information that an organisation is being actively targeted or may already be compromised.'[199]	private and public organisations to share information and intelligence on cyber-attacks.	ordinator for co-ordinated vulnerability disclosure. NIS 2 also establishes the Cyber Crisis Liaison Organisation Network, which will act as a cooperative network for the national authorities in Member States that are in charge of managing cyber crises. EU-CyCLONe will allow such authorities to collaborate and develop timely information sharing and situational awareness. eiDAS Regulation – Article 10 provides that where an electronic identification (e-ID) scheme notified by a member state to the Commission, or the online authentication of such a scheme, is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, then the notifying member state shall: • without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and • inform other member states and the Commission.[200]	communications, defence, emergency services, energy, finance, food, government, health, space, transport, and water.[203] The NCSC also provides advice and guidance on a broad range of cyber security related topics.[204] Additionally, the Cyber Security Information Sharing Partnership provides registered UK private sector organisations and government departments with a secure and confidential platform to share cyber threat information.[205] Other regulators also provide mechanisms for sharing information about cyber risks within the segments of the market that they regulate (e.g. the FCA and Ofcom).
	(b)	**Governance implications**	N/A	N/A	N/A	N/A	N/A
11	(a)	**Pending or new developments in cyber security regulation**	**Privacy Act Review Report** The Government released the Privacy Act Review Report in February 2023, which proposes significant changes to Australia's data privacy regime. Key proposals in relation to cyber security include: • introduction of a direct right of action (both individual and representative proceedings) for breach of the Privacy Act, • introduction of a maximum 72-hour period for notification of data breaches under the existing mandatory data breach	As set out above, in March 2022, Congress passed CIRCIA, which will create a reporting regime that applies to entities within critical infrastructure sectors. Also as above, the SEC issued draft regulations in March 2022 to enhance and standardise disclosures regarding cyber security incident reporting by public companies. Additionally, the SEC has also issued draft regulations that will require cyber security incidents' to be reported within 4 business days of reasonably concluding that an incident has occurred.[208]	As set out above, in 2022, the Canadian federal government introduced: • Bill C-26, which would (i) amend the *Telecommunications Act* to implement new cyber security obligations and (ii) enact the CCSPA, which would impose obligations on operators of "critical cyber systems"; and • Bill C-27, which would (i) enact the CPPA, which would replace PIPEDA with respect to obligations on safeguarding personal information and responding to breaches and would create a new	NIS 2 has already been adopted at the EU level. However, Member States have until 17 October 2024 to implement it on a national level, and this is when the majority of obligations under NIS 2 will commence in practice. DORA and the *DORA Amending Act* entered into force on 16 January 2023 but will not be directly effective until 17 January 2025, by which time all relevant entities will need to become compliant. **EU Cyber Resilience Act** Under the proposal for the EU Cyber Resilience Act, all products with digital elements placed on the EU market whose	The Data Protection and Digital Information Bill, which underwent the first reading speech in the House of Commons in late 2022, may: • narrow the definition of 'personal data' under the UK GDPR and the DPA,[212] • modify obligations to maintain adequate records, by removing the requirement for controllers to record all categories of data subjects and personal data and adding the requirement for controllers to record where personal data is stored,[213]

[199] *National Cyber security Strategy* (Report, March 2023) 16.
[200] eIDAS art 10.
[203] National Cyber Security Centre, 'CNI Hub'.
[204] National Cyber Security Centre, 'Advice & Guidance'.
[205] National Cyber Security Centre, 'Cyber Security Information Sharing Partnership (CiSP)'.
[208] Securities and Exchange Commission, 'Cyber security Risk Management, Strategy, Governance, and Incident Disclosure', (Proposed Rule, February 2022).
[212] Data Protection and Digital Information Bill Part 1(1) (***DPB***).
[213] DPB at [15].

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
		notification scheme, and a requirement to notify individuals as soon as practicable, • introduction of a baseline set of information security outcomes that organisations will be required to achieve through application of reasonable technical and organisations measures, and • a significantly broader range of enforcement mechanisms, including removal of the requirement for a breach to be 'serious or repeated' before a penalty is imposed. **SOCI Rules** The Security of Critical Infrastructure (Critical infrastructure risk management program) Rules[206] came into force on 17 February 2023. Responsible entities for certain critical infrastructure assets now have 6 months to take steps to adopt (and subsequently maintain) a critical infrastructure risk management program. CIRMPs must identify hazards where there is a material risk that the hazard could have a relevant impact on a critical infrastructure asset. **2023-2030 Australian Cyber Security Strategy** The Minister for Cyber Security recently announced the development of the 2023-2030 Australian Cyber Security Strategy with the aim of making Australia the most cyber secure nation in the world by 2030. **Other developments** The Cyber Security Industry Advisory Committee has also emphasised the increased risk of cyber security attacks in its 2022 Annual Report.[207]	In March 2023, the Biden administration announced a new cyber security strategy. Relevantly this strategy involves supporting 'legislative efforts to impose robust, clear limits on the ability to collect, use, transfer, and maintain personal data, and provide strong protections for sensitive data', as well as set national requirements to secure personal data consistent with standards and guidelines developed by the National Institute of Standards and Technology.[209] The strategy also involves developing legislation establishing liability for software products and services, preventing them from disclaiming disability by contract and establishing higher standards of care, including a safe harbour for companies that securely develop and maintain their software products and services.[210]	private right of action for affected individuals, (ii) establish an administrative tribunal to hear appeals of decisions made by the Privacy Commissioner of Canada and apply a new administrative monetary penalty regime, and (iii) enact the *Artificial Intelligence and Data Act* to regulate international and interprovincial trade and commerce in artificial intelligence systems.	intended and reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network would need to carry a CE marking which demonstrates that they meet a minimum standard of cyber security. The proposed *Cyber Resilience Act* will place obligations on a range of economic operators in the supply chain, with the most onerous obligations being placed on manufacturers. **EU Artificial Intelligence Regulation (AI Act)[211]** The proposed AI Act will regulate AI systems that have an element of autonomy. As part of the proposals, such systems will be classified according to their risk, with the higher risk systems either being prohibited or subject to conformity assessment and risk management procedures that will include security requirements. Incidents or malfunctions in high risk systems will also need to be notified to competent supervisory authorities. The risk categories will likely be as follows: • unacceptable-risk, • high-risk, • limited risk, and • minimal-risk. Unacceptable-risk systems may include: • systems that use subliminal techniques in a manner likely to cause physical or psychological harm, • social scoring systems generally, for example by using AI to evaluate an individual's trustworthiness based on social behaviour, • systems that exploit vulnerable people due to their age,	• remove the requirement in some instances to conduct assessments of 'high-risk data processing',[214] • replace the Information Commissioner with an Information Commission, and[215] • give the Information commission power to compel companies to produce a report and attend interviews.[216] The UK government has also announced that it will amend UK NIS. See row 2(a) above for more information.

[206] (LIN 23/006) 2023 (***CIRMP Rules***).

[207] Cyber Security Industry Advisory Committee, 'Australia's Cyber Security Strategy 2020', Annual Report (2022).

[209] *National Cyber security Strategy* (Report, March 2023) 20.

[210] *National Cyber security Strategy* (Report, March 2023) 21.

[211] Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts.

[214] DPB at [17].

[215] DPB part 5.

[216] DPB at [35], [36].

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
					disability, or specific social or economic situation, and • 'real-time' biometric identification systems used in public spaces by or on behalf of law enforcement. These systems will likely not be permitted in the European Union, subject to limited exceptions. High-risk systems may include: • AI systems used as safety components in products that are subject to EU harmonisation legislation and which require third party conformity assessment under such legislation, and • AI systems used for certain prescribed purposes in specific areas, such as remote biometric identification systems used in non-public spaces, AI systems used as safety components for critical infrastructure, and systems used in educational and vocational training, employment, the provision of essential services, law enforcement, and the justice and democratic system. Providers of high-risk systems will be subject to a number of requirements, which may include: • the establishment of a risk management system to identify and evaluate associated risks as well as adoption of suitable risk management measures, • adherence to data governance and management requirements, particularly for data used to train AI systems, • drafting of technical documentation to a minimum level of detail (to be retained for a minimum period), • designing the systems to include automatic record-keeping of events (logs), • designing the systems to have an appropriate level of accuracy, robustness and cyber security, • ensuring the systems have appropriate human oversight,	

#	REGULATORY AREA	AUSTRALIA	US (FEDERAL)	CANADA (FEDERAL)	EU[14]	UK
					including the ability for a human to override the system, and • requirements to perform a conformity assessment to demonstrate compliance with the AI Act, and to keep a signed declaration of conformity. In addition to the above, providers of high-risk AI systems may also have the following obligations: • implementing a 'quality management system' that includes a strategy for regulatory compliance and an accountability framework setting out the responsibilities of management and staff for the system, and • informing national competent authorities about serious incidents or malfunctions that constitute a breach of fundamental rights, as well as any recalls or withdrawals of AI systems from the market.	