pwc.com.au/cybersecurity

Strengthening Australia's Security Regulations and Incentives Consultation Paper

PwC Public Submission

August 2021

pwc

Contents

Executive Summary 3

Why Should Government Take Action? 5

The Current Regulatory Framework 7

Governance Standards for Large Businesses 10

Minimum Standards for Personal Information 12

Labelling for Smart Devices 14

Clear Legal Remedies for Consumers 17

Contacts 19

Executive Summary

The Strengthening Australia's Cyber Security Regulations and Incentives Discussion Paper (the Discussion Paper) seeks industry input to a number of questions arising from previous engagement in the development of Australia's Cyber Security Strategy 2020. PwC Australia (PwC) provided a submission to that in November 2019. This submission provides PwC's commentary on a range of the questions outlined in, and broadly follows, the structure of the Discussion Paper.

Our purpose is to build trust in society and solve important problems and we are committed to driving Australia's cyber partnership effort to mitigate and reduce risks to our national security and economic recovery from large scale sophisticated cyber threats. Through our role as an advisor to the Australian government's Cyber Security Strategy Industry Advisory Committee, we see first hand the cyber threat challenges facing the country and actively provide our expertise to help design solutions to mitigate these critical risks.

Our submission provides our view on Discussion paper topics important in developing a considered framework for regulating and securing Australian businesses and consumers. Our key observations and recommendations include:

There are opportunities for the harmonisation of legislation and standards to reduce the areas of duplication or inconsistencies between competing legislation and standards. This will, in turn, provide greater confidence for businesses and organisations to address cyber threats without the task becoming a regulatory compliance burden. Adopting a national approach, aligned with national security policies and allowing cross-sectoral fertilisation and capacity building should be considered. Equally, we see there is opportunity for Australia to play a stronger role in the development and harmonisation of international standards. As a globally integrated economy we are well placed to input into the evolution of frameworks that seek to mitigate cyber risks.

While best practice guidance will certainly assist organisations, changes to director obligations and mandatory governance requirements may not achieve behaviour change and drive the desired outcomes. A voluntary framework may provide an appropriate and objective baseline to assist cyber resilience uplift. Stronger governance within particular industries may create a positive impact more broadly. This may be an alternative way to create the right incentives while avoiding the need for additional regulation. Further consultation will be required on these standards and the organisations subject to them.

	Enhanced education for directors and owners of small and medium companies and easy to find supporting information about existing support could improve confidence across this part of the economy. This could be achieved through broadening foundational and continuing professional development courses for directors, such as those offered by the Australian Institute of Company Directors (A.I.C.D), to include a greater focus on cyber security and digital risk. In addition to improving education and support, tax incentives to increase security posture and mobilise preventative security measures may serve as incentive to implement better cyber security practices. Further, as the borders reopen to skilled migration, governments and businesses should consider prioritisation and incentives to encourage cyber professionals to relocate to Australia, given the current shortage of skills and capabilities in the market.
	The cost effectiveness of implementing cyber security controls should be considered by businesses in the light of how they can overall reduce cost and increase competitiveness. Messaging from government to business about implementing these controls might beneficially point out the need to consider the costs as an investment that should be made in order to achieve these types of returns. Defining the problem by quantifying the business impact rather than using technical or security language may assist to encourage businesses to implement security best practices. Additionally, we believe there is a need to encourage Boards in Australia to further consider how they get assurance over the effectiveness of the controls that are put in place to manage their cyber risks. Independent assurance reviews that focus on the business impact could be a valuable tool for businesses seeking confidence in their implemented controls.
	A standardised cyber security framework for smart devices that is digestible for all levels of tech-literacy would promote consumer confidence. The framework would provide manufacturers with a set of guidelines to assist with the design and manufacturing of their products and could provide them with a competitive edge over less secure devices.
	Legal remedies and reforms should be considered as holistically as possible, to ensure the cyber regulatory environment becomes more harmonised. The Government is already aware that the right balance needs to be adopted to ensure legislative reforms being proposed and implemented under the various legislative regimes do not become a burdensome compliance task for businesses, thereby impacting innovation and entry to market. This needs to remain a priority as any regulatory changes are considered.

PwC has incorporated inclusive design into this paper, with the view to promote accessibility for all Australians. This includes practically embedding accessible web document practices into the paper itself (e.g. accessible acronyms for digital screen readers).

Why Should Government Take Action?

The Discussion Paper seeks views on factors preventing the adoption of cyber security best practice in Australia in order to identify some of the core drivers of current cyber security challenges and determine an appropriate role for Government.

Since the introduction of the Australian Government's Cyber Security Strategy 2016 and its update in 2020 there has been significant change across the cyber security landscape. Efforts by Federal, State and Territory governments to raise awareness and improve resilience of individuals, businesses and educational organisations are being supported by a growing number of larger organisations. Recognition that cyber security is critical to an organisation is growing. PwC's 24th Annual Global CEO Survey[1] showed 95% of Australian CEOs see cyber risk as the top threat to business growth while at the same time only 78% are increasing long term investment into cyber security and privacy or including cyber threats in strategic risk management activities.

The survey also points to some factors that impact the ability of organisations to adopt cyber security best practices. It showed about a quarter of Australian CEOs think their organisations need to do more to measure and report on cyber security and data privacy. However, in order to increase measurement and reporting, organisations must be able to explain cyber risk in a way that successfully engages decision makers and investors, to relate cyber risk to business outcomes. This points to a continued need to educate decision makers and investors about cyber risk and the value of implementing cyber security best practices.

While a lack of understanding of the link between cyber risk and business outcomes is a clear factor preventing implementation of cyber security best practices, there are other factors at play across the economy. Individuals and businesses will always make risk assessments when determining the need to spend time or money on implementing mitigations. This is no different in the context of cyber security. In many cases, regardless of the growing awareness of cyber threats and their impacts, individuals and those in small business may not recognise their threat exposure nor understand the consequences of a data breach or cyber attack. In these cases, the cost of adopting best practice may seem prohibitive and the effort inconvenient. Similarly, cyber security practices that seem to reduce efficiency, or are perceived as difficult to either implement or use, are likely to be subject to workarounds and thus become ineffective.

Additionally, the innovation and agility required to compete in today's modern knowledge economy often necessitates rapid development and subsequent fielding of technologies which have not been developed with cyber security as a primary concern. This behaviour is amplified by the lack of incentives to implement security by design and the corresponding DevSecOps

[1] https://www.pwc.com.au/ceo-agenda/ceo-survey.html

(Development, Security and Operations) resources, as these principles are perceived to hinder innovation and increase costs. Additional government regulation and involvement to encourage changes in these behaviours may be effective to address this. However, any such effort must also balance the need to compete internationally and continue to encourage innovation without increasing bureaucracy or slowing prototyping and subsequent deployment time to market.

Cyber security exists in a global ecosystem impacted by national and international government regulation in addition to market forces. Negative externalities and information asymmetries arise in this environment through the different drivers between local markets. For example, the rise of mainstream social platforms would be very different if they were Australian companies. The Privacy Act and local market regulations would influence such a company differently to its development in the United States. Cyber security regulation must balance the requirement for local companies to compete on a level playing field against international competitors. If additional security regulations are developed, they must be balanced with this competitive nature in mind. Otherwise, Australia could have very secure products which cannot compete unless consumers of such products are willing to pay the necessary premium and accept a slower delivery to market of these more secure products.

PwC Australia are actively engaged in works to align local and global approaches to managing cyber security risk, influencing both the development of international cyber standards, for example as Advisory Contributors to Version 2 of the Cyber security Capability Maturity Model, and in the alignment of local Australian frameworks, such as the Australian Energy Sector Cyber Security Framework. We believe it is important for the Government to continue to seek alignment between local and global approaches to managing cyber security risk.

The Current Regulatory Framework

Strengths and limitations of the current cyber security regulatory framework

Australia's current cyber security regulatory framework has many strengths. Key strengths include:

Government prioritisation

The prioritisation of cyber security by the Federal government and regulators as an important matter for Australia's national security, innovation and prosperity. This focus from the top demonstrates a willingness for policy makers and regulators to change and evolve regulatory settings quickly, efficiently and effectively as cyber threats change.

Distributed responsibilities

The number of shared responsibilities across government agencies (eg. Department of Foreign Affairs and Trade, Defence, Department of Home Affairs, and State/Territory governments) helps to ensure there is a multi-pronged approach to addressing cyber threats and protecting Australians.

Collaborative contribution

The collaborative spirit of those that contribute to the framework. The overall framework is not dominated by a particular bureaucracy, instead led by a broad family of intelligence agencies, industry, regulators and government.

Limitations of the current regulatory framework include:

Fragmentation across jurisdictions: The current regulatory framework does not deal coherently with the spread of the cyber security ecosystem across multiple jurisdictions. The nature of working in a connected world makes it difficult to design cyber regulation when the cyber ecosystem of so many businesses is spread across different jurisdictions. In the context of the risk to Australia's economy, communities and national security, this part of the current regulatory framework for cyber security appears to be under-developed.

Multiple governing legislative and regulatory instruments: Cyber security in Australia is governed by a series of Commonwealth and State-based legislative and regulatory instruments which are each enforced by different bodies. For example:

- Federal and State criminal laws (eg. *Crimes Act 1914* (Cth), *Criminal Code Act 1995* (Cth), *Crimes Act 1900* (N.S.W.))

- obligations to take all reasonable steps to protect personal information and have a breach response under the *Privacy Act* 1988 (Cth);
- the possibility for Ministerial directions under the *Security of Critical Infrastructure Act* 2018 (Cth);
- the *Telecommunications (Interception and Access) Act 1979* (Cth) which requires telecommunication services to collect and retain specific types of data and comply with the Privacy Act in relation to that data; and
- the requirements in the Australian Prudential Regulation Authority Prudential Standard CPS234.

The differences in approaches between Federal and State governments to dealing with COVID highlights some of the issues faced when there are multiple governing agencies dealing with an issue.

Fragmentation across regulatory bodies: Regulatory enforcement roles are similarly fragmented. Some of the key cyber security regulatory bodies include Australian Signals Directorate, Australian Cyber Security Centre (A.C.S.C), Department of Home Affairs and Critical Infrastructure Centre. While the different bodies collaborate and coordinate efforts, there is a weakness inherent in a non centralised, federated style structure for regulation of cyber security.

Regulatory environment evolution

Current limitations in the regulatory environment for cyber security could be strengthened through:

Harmonisation of legislation and standards

There are opportunities to reduce the areas of duplication or inconsistencies between competing legislation/standards which will in turn provide greater confidence for businesses and organisations to address cyber threats without the task becoming a regulatory compliance burden. There is merit in adopting a national approach, aligned with national security policies and allowing cross-sectoral fertilisation and capacity building. Equally Australia should seek to influence the development of international standards to ensure they take into account the Australian risk landscape and to promote harmonisation in standards across globally integrated economies.

Clarity of Obligation

More prescriptive regulatory frameworks may assist organisations in providing a consistency of approach. This clarity may benefit participants by allowing them to know at the outset the cyber security standard they are required to meet.

Regulatory roles and resourcing

The roles of the many regulators can be seen by some stakeholders as confusing and fragmented. Some possible options to consider include the following:

- The Critical Infrastructure Centre, which sits within the Commonwealth Department of Home Affairs, has an existing regulatory role in relation to cyber security in the telecommunications sector and exposure to certain sectors through the *Security of Critical Infrastructure Act* 2018 (Cth). These capabilities could be expanded to include the regulation of the broader economy's cyber security.
- Some sector regulators may be well placed to administer a sector wide regulatory regime regarding cyber security. Their industry expertise and resources will improve coverage and enforcement of cyber security requirements. However, it would also require their technical expertise to be expanded in order to support this.
- Regulators should have strong enforcement powers, appropriate levels of resourcing to support their works, and active compliance and audit functions. The current level of resourcing available to the regulators (and competing priorities for some) is disparate. The differences in resourcing impacts on the activities and responsiveness of the regulator to address cyber and enforce compliance.
- The effectiveness of a decentralised model is dependent on all the regulators working together and agreeing on a harmonised or consistent approach to tackling cyber security challenges.

Governance Standards for Large Businesses

Approaches to strengthen corporate governance of cyber security risk

The Corporations Act (and other common law obligations) provide a robust set of director duties. Duties that are successfully applied to meet different challenges in the Australian corporate landscape.

It must be acknowledged however, that Boards and executive management teams may need guidance on baseline standards. Voluntary standards or best practice guidelines may therefore be helpful in assisting with cyber resilience uplift.

While cyber risks create some new challenges, it does not seem necessary or appropriate to consider reforms that may introduce additional director duties or mandatory standards. With the right guidance, the current regulatory framework should be sufficient.

There are a number of issues that still need to be considered as part of the proposed options. It is difficult to understand whether the voluntary guidelines proposed are intended for management or Boards. While Boards will need to critique and assess their management teams, the voluntary guidelines appear more appropriate to guide a company's management team.

It is also challenging to assess the merits of any voluntary framework without an understanding of the content. In many respects, it appears that the proposal is looking to address gaps left by the critical infrastructure reforms. That is, picking up large businesses that are not already caught by the proposed reform agenda. This raises questions about the applicability of different standards and the complexity with defining "large business". We recommend further consultation on these matters.

We note, stronger governance within particular industries may create a positive impact more broadly. This may be an alternative way to create the right incentives while avoiding the need for additional regulation.

Support for directors of small and medium companies

Enhanced education for directors and owners of small and medium companies, and easy to find supporting information about existing support, may further improve confidence in cyber resilience uplift. Appropriately targeted support by the A.C.S.C to help businesses prepare for, and recover from, a cyber security incident may also facilitate improved resilience. Often it is not about an unwillingness to improve, but about knowledge of how to improve and what constitutes "best practice". Comparisons within industries may create a misplaced level of comfort if a more objective assessment demonstrates shortcomings.

In addition to improving education and support, tax incentives to increase security posture and mobilise preventative security measures may serve as incentive to implement better cyber security practices.

Senior business leader education and awareness

The A.I.C.D incorporates mandatory training modules on cyber security and cyber risk within the A.I.C.D course[2]. The current focus of these training modules is centered around the Privacy Act, so there would be benefits in expanding the scope.

Another approach could be to consider the current cyber capabilities of the board. Should cyber skills and awareness be lacking, consider incorporating cyber security expertise into board governance, as recommended in principle 5 of the World Economic Forum's Principles for Board Governance on Cyber Risk.

[2] https://aicd.companydirectors.com.au/membership/membership-update/six-principles-for-boards-on-cyber-risk-governance

Minimum Standards for Personal Information

An Approach for promoting the uptake of cyber security standards

The Privacy Act in its current form may not be the best place to house a cyber security code. The current scope of the Privacy Act covers personal information, government entities and Australian Privacy Principle (A.P.P) entities only. From a cyber perspective, this is narrow and does not cover the full ambit and scope of entities and data that may be subject to cyber threats.

Whilst reforms are being proposed to extend the definition of 'personal information', the application of the Privacy Act is still limited and would not sufficiently cover the wide ambit of data that is at risk of cyber attacks. It does not, for example, cover Intellectual Property or other commercially or otherwise valuable data which are significant cyber theft targets.

If such a code is to be housed under the Privacy Act, and therefore under the responsibility of the Office of the Australian Information Commissioner (O.A.I.C), substantive reform would be needed to support the success of the code, including:

- the potential need to change the title of the Privacy Act to better reflect the wider scope;
- expansion of the application of the Privacy Act and therefore the code by the removal of current thresholds;
- the ability for Ministerial directions etc to be made to enable and quickly respond to emerging cyber threats and evolving technologies;
- substantive increases in resourcing, powers, and expertise for the O.A.I.C.

While regulated entities may wish to obtain certainty as to when they have 'implemented' everything that is required to take 'reasonable steps' to protect personal information as per A.P.P 11 and manage liability risks, there are several negative consequences to taking this approach that would need to be considered:

1. Reasonable steps should be informed by, and proportionate to, the risks the organisation faces, not based on a compliance-driven approach. Compliance-driven approaches may encourage investment in less efficient cyber controls that do not specifically address actual risks to the confidentiality of personal information. Determination of the cyber security measures needed should be based on a robust assessment of the particular risks an organisation faces and the assets it needs to protect. Encouraging business leaders to assess what their 'crown jewels' data assets are and assessing measures to protect those rather than a generic compliance or 'tick box' approach is needed.

2. Cyber security moves rapidly, in response to the evolving techniques adopted by threat actors and novel technologies entering the marketplace. A cyber code under the Privacy Act may not be maintained in a sufficiently responsive way to keep pace with the flux seen in cyber practices.

3. It is unnecessary to create a separate information security compliance framework dedicated to protecting personal information. This would add further complexity to an already fragmented regulatory space, where many organisations already struggle to meet multiple (sometimes conflicting) data protection and cyber security compliance requirements that originate in legislation, sectoral regulations, industry frameworks or from international jurisdictions.

4. There are already a number of authoritative information references produced by leading Australian agencies to provide advice on better practices, such as the A.C.S.C's 'Cyber Security Principles', Essential 8 and detailed Information Security Manual Guidelines. The O.A.I.C also publishes recommendations on better practices for maintaining compliance with A.P.P 11. These guidelines and references are updated on a regular basis to keep pace with emerging threats and drive improvement across industries. Furthermore, these guidelines apply to any type of information requiring protection, not just personal information.

Cost effective and achievable technical controls

Cost effectiveness of cyber controls would generally need to be assessed on a case-by-case basis. There are few controls for which the associated cost would not be closely linked to an organisation's specific technology and business environment.

The A.C.S.C's Essential 8 establishes a minimum standard for Government agencies which should be considered by all businesses.

Implementing the controls set out by the essential 8 would benefit businesses in protecting their intellectual property and customer data by establishing a solid baseline for cyber security controls.

In addition to increasing their security posture, there would be beneficial flow on effects for businesses, such as decreased cyber security insurance fees and potentially endorsement or certification from an Australian regulatory body that the business meets the minimum security requirements to protect user information. Such endorsement may improve business reputation and have enhanced competitive advantage.

The cost effectiveness of implementing these controls should be considered by business in the light of such reduced cost and increased competitiveness. Messaging from government to business about implementing these controls might beneficially point out the need to consider the costs as an investment that should be made in order to achieve these types of returns. Defining the problem in business, return-on-investment language rather than technical or security language may assist to encourage businesses to implement security best practices.

Labelling for Smart Devices

Encouraging the purchasing of secure smart devices

Research suggests consumers are generally anxious that their privacy and security will be at risk when they use smart home devices. Consumers also believe the impact of a privacy breach to be significant as opposed to low[3].

Proof of cyber security and low risk to privacy breaches will be key in persuading consumers to purchase smart devices and technology. This is particularly the case where children's access to and ownership of devices is also increasing[4]. Thus, some form of standardised independent assessment would likely increase consumer confidence, much like how energy efficiency and health nutritional values are assessed and communicated.

There is also a disconnect between consumer concerns and how business communicates benefits of smart devices. Business overly focuses on convenience and economy concerns, while consumers (particularly older ones) are largely concerned with privacy and data security. Greater emphasis on cyber security in advertising and education is something that may bridge this disconnect. In addition, some standardisation and consistency in, for example a star rating system, might help provide consumers with an easily recognisable and consistent standard to rely upon to make their consumer choices on cyber and privacy expectations.

Research demonstrated that with the exception of a label that implied weak security, participants were significantly more likely to select a device that carried a label than one that did not. While they were generally willing to pay the most for premium functionality, for two of the labels tested, they were prepared to pay the same for security and functionality. Qualitative responses suggested that participants would use a label to inform purchasing decisions, and that the labels did not generate a false sense of security[5].

Introducing a Government rebate for smart device companies to adopt the labeling scheme could assist in accelerating the uptake.

---

3 https://www.sciencedaily.com/releases/2020/08/200804111449.htm

4 O.A.I.C. Australian Community Attitudes To Privacy Survey 2020

5 https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0227800

Implementing a cyber security framework for smart devices

A standardised cyber security framework for smart devices that is digestible for all levels of tech-literacy would promote consumer confidence. The framework would also provide manufacturers with a set of guidelines to assist with the design and manufacturing of their products. This approach will assist in alleviating consumer anxiety over privacy and data concerns.

Standards to be introduced and adopted will need to be balanced as it should not become an over-compliance burden especially on smaller players and new entrants in the market, which may stifle competition, innovation, and limit consumer choice and options.

Ensuring industry support and uptake

Industry support, update and uptake would be conditional on an independent assessor and watchdog as well as effective regulation. The Australian Consumer Laws may apply to ensure manufacturers do not make false or misleading representations in using voluntary labels.

Manufacturers who are able to demonstrate high security standards would welcome a labelling system as it could give them a competitive edge over less secure devices. Where manufacturers are not able to demonstrate a high security level, a decrease in their sales would directly improve the nation's collective cyber security posture.

Recommended labelling scheme

Australia should consider Singapore's experience following the launch of its Cybersecurity Labelling Scheme (C.L.S)[6] for consumer smart devices to improve security, raise overall cyber hygiene levels and better secure Singapore's cyberspace for Internet of Things (I.o.T) devices.

Under the scheme, cyber security provisions will be displayed on smart devices which will enable consumers to make informed decisions when selecting products. A key aim of the C.L.S is to assist manufacturers to differentiate themselves from their competitors and to encourage the development of more secure products. Historically, smart device manufacturers have primarily focused on features, functionality and cost.

Wi-Fi routers and smart home hubs were prioritised by the C.L.S due to their wide usage as well as the impact that a compromise of the products could have on users. The scheme has been recently extended to include all categories of consumer I.o.T devices, such as I.P cameras, smart door locks, smart lights and smart printers.

6 https://www.csa.gov.sg/Programmes/cyber security-labelling/about-cls

To encourage adoption of the scheme, the Cyber Security Agency of Singapore is waiving the application fees for the C.L.S for one year until 6 October 2021.

The most pragmatic approach to a smart device expiry would be to have the device expire once the manufacturer ceases security patch releases for that particular model. However, the ability to pre-determine an expiry date on devices is constrained by the very aspects that challenge the security of technology more broadly. Market forces and innovation will cause device producers to make decisions about the lifespan of devices and thus security patch releases. A standard lifespan for devices is not possible to define.

A more effective approach may be to label devices according to the security standards they meet at the time of placement in the market with a warning to consumers that this is a point in time rating only. A potential solution is to have physical labelling on the packaging and/or device for sale and have an updatable digital register for smart devices. The digital register can keep track of patches and security updates, as well as when a product is no longer supported.

Physical labels with a QR scan code for example which links to the digital register may be an option.

Inclusion of mobile phones in the labelling scheme

As smartphones are the primary method of interfacing with home smart devices and with the Internet of Things it seems logical that they would be included in the scheme. The United Kingdom decided to include smartphones into its scheme while Singapore has opted not to include mobile phones. Smart devices store a substantial amount of personal and other information and are used extensively in everyday life, this makes them attractive targets for potential cyber criminals and hackers.

Clear Legal Remedies for Consumers

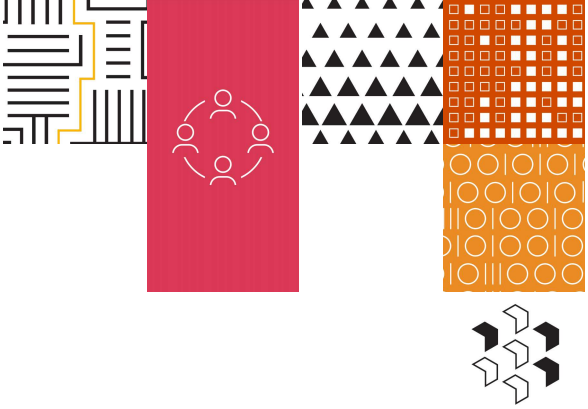
Identified Consumer Law gaps relating to cyber security risk

Over the years, the limitations of the Australian Consumer Laws in terms of its application to digital products, digital platforms and emerging technologies have been exposed. The Australian Competition and Consumer Commission's Digital Platforms Inquiry Report further highlighted the limitations of the Australian Consumer Law to addressing certain practices (ie. dark patterns) by digital platforms.

Further, despite the threshold limit to a 'consumer' being recently increased, the Australian Consumer Law largely governs the supply of goods and services to consumers and small businesses. The definition of 'goods' in the Competition and Consumer Act was amended to include 'computer software' but there is debate as to whether this includes e-books and digital music and other digital content in Australia. In the United Kingdom, it is clear that consumer protection laws apply also to the supply of digital content.

In the absence of a private right of action to address privacy compromises and intrusions, consumers need to have appropriate legal remedies if they fall victim to cyber or data breaches. Several law reform commissions have raised the question of introducing a statutory tort of privacy, being a statutory cause of action for serious invasions of privacy. The Australian Competition and Consumer Commission also recommended the introduction of such a cause of action in its Digital Platforms Inquiry Report.

Given the rapid evolution of digitisation, along with a very dynamic cyber risk profile, it is not surprising that there may be gaps in the legal framework that seek to mitigate consumer harm. We observe that Section 18 of the Australian Consumer Law, which broadly prohibits a person, in trade or commerce, from engaging in misleading or deceptive conduct, may expose a business to a claim that a company / individual has misrepresented cyber posture.



Reform Considerations

There are significant areas of reform currently being explored, from reforms to expand the Privacy Act, extension of those impacted by the Security of Critical Infrastructure Act 2018 to regulatory options to address the growing threat of ransomware. All reforms currently being explored are valuable and will work toward making a step change to mitigate cyber risks.

Our key recommendation is that reforms are considered as holistically as possible, to ensure the cyber regulatory environment becomes more harmonised. The right balance needs to be adopted to ensure legislative reforms being proposed and implemented under the various legislative regimes do not become a burdensome compliance task for businesses, thereby impacting innovation and entry to market.

Contacts

Pip Wyrdeman
Partner, Cyber Security
& Digital Trust
[redacted]

Cameron Whittfield
Partner, Cyber Security
& Digital Trust
[redacted]

Further information about PwC Cyber can be found at
https://www.pwc.com.au/important-problems/cyber-security-digital-trust.html

pwc.com.au/cybersecurity

WLT127083071