Getting regulation right

Approaches to improving Australia's cybersecurity

Rajiv Shah

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Policy Brief
Report No. 73/2023

About the author

Dr Rajiv Shah is a Fellow at ASPI's Cyber, Technology and Security. He has worked in the cybersecurity and technology business for more than 20 years, over which time he has seen the internet evolve from an academic curiosity to today's hyperconnected world. He has held a broad range of senior leadership roles with major multinational technology companies and now also leads his own consulting business, MDR Security, providing expert advisory services to government and businesses to solve their most complex challenges in cyber security, data and digital transformation. He is also a regular speaker at industry conferences and contributor to industry publications.

Rajiv's experience has spanned a broad range of business and technical domains, with roles that have included business analysis, technical architecture, program delivery, operational management, strategy, business transformation, client relationship management and more. He has spent time working in the UK and the US, and since 2011 has been based in Canberra, Australia. Before joining the commercial world, Rajiv completed a PhD in quantum physics and retains a keen interest in mathematics and science

Acknowledgements

ASPI acknowledges the Ngunnawal and Ngambri peoples, who are the traditional owners and custodians of the land upon which this work was prepared, and their continuing connection to land, waters and community. We pay our respects to their cultures, country and elders past, present and emerging.

The author would like to thank all the stakeholders across government and commercial sectors who generously made their time available for consultation discussions, the ASPI staff who reviewed the work and supported this project, in particular Vahri Fotheringham, Jocellin Kang and Alex Caples, and the external reviewers whose feedback was invaluable in the finalisation of this report.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our annual report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements.

ASPI Cyber, Technology & Security

ASPI's Cyber, Technology and Security (CTS) analysts aim to inform and influence policy debates in the Indo-Pacific through original, rigorous and data-driven research. CTS remains a leading voice in global debates on cyber, emerging and critical technologies, foreign interference and issues related to information operations and disinformation. CTS has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building and Internet safety, satellite analysis, surveillance and China-related issues. To develop capability in Australia and across the Indo-Pacific region, CTS has a capacity building team that conducts workshops, training programs and large-scale exercises for the public, private and civil society sectors. Current projects are focusing on capacity building in Southeast Asia and the Pacific Islands region, across a wide range of topics. CTS enriches regional debate by collaborating with civil society groups from around the world and by bringing leading global experts to Australia through our international fellowship program. We thank all of those who support and contribute to CTS with their time, intellect and passion for the topics we work on. If you would like to support the work of the CTS, contact: ctspartnerships@aspi.org.au.

Important disclaimer

ASPI

Tel Canberra: +61 2 6270 5100
Tel Washington DC: +1 202 414 7353
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_CTS

First published August 2023. ISSN 2209-9689 (online). ISSN 2209-9670 (print).

Cover image: iStockphoto.com/BrianAJackson.

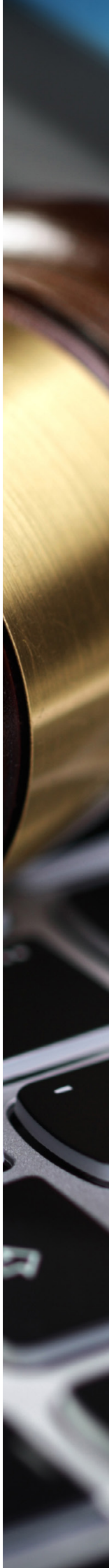
ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Funding for this report was provided by Microsoft.

Getting regulation right

Approaches to improving Australia's cybersecurity

Rajiv Shah



Policy Brief
Report No. 73/2023

Contents

What's the problem?

As well as having a global impact, Cybersecurity is one of the most significant issues affecting Australia's economy and national security. On the one hand, poor cybersecurity presents a risk to the interconnected digital systems on which we increasingly rely; on the other hand, well-managed cybersecurity provides an opportunity to build trust and advantage by accelerating digital transformation. Cyber threats can originate from a diverse range of sources and require a diverse set of actions to effectively mitigate them. However, a common theme is that much better cyber risk management is needed to address this critical threat; the current operation of the free market isn't consistently driving all of the required behaviours or actions.

Regulation can provide a powerful mechanism to modify incentives and change behaviours. However, securing cyberspace depends on the intersection of many factors—technical, social and economic. Current regulations are a patchwork of general, cyber-specific and sector-specific measures with a lack of cohesion that causes overlaps and gaps. That makes the environment complex, which means that finding the right approach that will truly improve overall security and minimise unwanted side effects is difficult. It's necessary to analyse the interconnected factors that determine the net effectiveness of cybersecurity regulations.

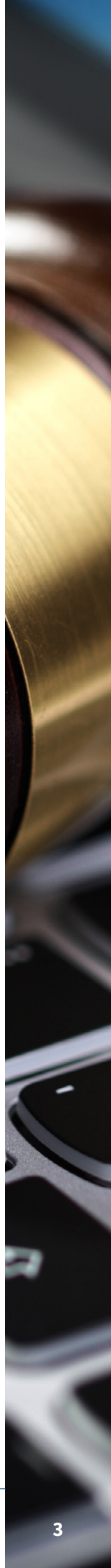
Furthermore, the pace of technological change is so fast today that, even if regulation is successful when first implemented, it needs to be appropriately futureproofed to avoid becoming irrelevant after even a few months. Recent rapid developments in artificial intelligence are an example of the risks here that will need to be anticipated in any changes to the regulatory regimes.

What's the solution?

Regulatory interventions have an important role to play as one part of a strategy to uplift Australia's cybersecurity, if done in the right way. This paper presents a framework for the government to make appropriate decisions about whether and how to regulate. That must start with defining which aspect of the cybersecurity challenge it seeks to address and the specific intended long-term impact. In cybersecurity, the most appropriate metrics or measures that regulation seeks to influence should, where possible, be risk-based, rather than specific technical measures. This is because the actual technical measures required are dependent on the individual context of each situation, will change over time, and are effective only when combined with people and process measures. The impact of the interventions on those metrics needs to be readily measurable in order to enable reliable enforcement at acceptable cost—both direct financial cost and indirect opportunity costs.

There's often a focus on regulation to compel entities to do or not do something. However, compulsion is only one form of regulation, and others, such as facilitation or encouragement, should be considered first, treating compulsion as only one possible approach, which should used carefully and strategically.

Detailed implementation of cybersecurity regulations should use a co-design process with the relevant stakeholders, who will bring perspectives, experiences and knowledge that government alone does not have. It should also draw upon relevant experience of international partners, not only to benefit from lessons learned, but also to minimise the compliance burden for global companies and operators. Finally, in recognising the complexity of the problem, an iterative approach that measures impact and adjusts approaches to enhance effectiveness, incorporate lessons learned and absorb technological advances needs to be planned from the outset.



Introduction

Today, so much of Australia's economic prosperity and national security is critically dependent on digital infrastructure and assets. Increasingly, everyday activities such as banking, communication and navigation are wholly dependent on the availability of internet connectivity, so those networks are underpinning virtually all exchanges of sensitive and critical data. At the same time, cyberattacks on digital infrastructure have become more commonplace and sophisticated. The sources of the attacks include a diverse range of groups with different motivations and approaches; however, a common theme is that Australia needs much stronger cyber risk management in order to address what's becoming a critical threat to the nation's security and prosperity.

The Australian Government has recognised this challenge and is in the process of developing a new national cybersecurity strategy, which is due out later this year.[1] The digital infrastructure and assets that the strategy will need to cover are many and diverse and are a mixture of private and public ownership and responsibility. Even if the government had the inclination to take responsibility for securing everything, it lacks the budgets, skills and resources to directly do so. Therefore, the upcoming strategy will need to take a collective approach, combining direct government action with measures that encourage action by other stakeholders to drive security improvements. Regulation will be a key potential lever to modify the behaviour of stakeholders, encouraging them to implement the desired actions that will uplift the overall cybersecurity of the nation.

There's no doubt that regulation can be a powerful lever, but effective pull-through is complex, requiring a number of stages from implementation through to modifying the directly targeted outputs, to delivering initial outcomes, to making the desired long-term impact. There are many assumptions and dependencies to be validated and managed by government in the design and implementation of the regulations in order to deliver that pull-through. There's always a significant risk of modifying the behaviour of stakeholders in unintended ways, leading to unwanted consequences that can offset or even eliminate any direct benefits delivered.

The aim of this paper is to analyse the interconnected factors that determine the net effectiveness of cybersecurity regulations. The analysis draws upon research of open-source material, interviews with key stakeholders in government, local industry and multinational technology providers, and a roundtable discussion convened by ASPI of a cross-section of stakeholders. Those inputs and analysis are used to provide recommendations for where and how such regulations can be used as part of an integrated strategy, to help maximise the cybersecurity benefits while minimising costs and other unwanted impacts.

This paper starts with a consideration of the current Australian context, including some of the regulatory initiatives already underway, and then consider the broader international context. It then introduces a framework for defining different potential approaches and use it to identify issues and propose recommendations for government.

The Australian regulatory landscape

Overview of current state

Cybersecurity regulation in Australia today is split across several different regulatory mechanisms administered by different government departments. Cybersecurity is just one aspect of risk and security, and therefore, as well as cyber-specific regulations, cybersecurity is effectively included in a range of other different regulations. Many of those other regulations pre-date the modern digital era and hence weren't necessarily created with cyberspace, cybersecurity concerns or technological innovation front of mind.

Table 1 on the following page summarises the main regulations that are relevant to cybersecurity, which are then discussed in more detail below, followed by a consideration of some of the effects of this overall patchwork and the consequent lack of cohesion. This section then concludes with a review of currently announced relevant regulatory initiatives.

Cybersecurity-specific regulations

Cybersecurity-specific regulations have generally been sector-based to date, reflecting a risk calculus approach by government to target the greatest areas of concern and resulting in uneven regulation as the technology landscape and ways of working have evolved.

Telecommunications networks have long been identified as a critical sector, given both the sensitivity of some of the data they carry and the importance of their availability to the effective functioning of modern digital society. The *Telecommunications Sector Security Reforms* (TSSR)[2] came into force on 18 September 2018 and place obligations on providers to protect their networks with 'competent supervision' and 'effective control' over them, and the requirement to notify the government of any planned changes that could affect those obligations. The TSSR also provide the government with powers to gather information on telecommunications networks to monitor compliance with those obligations and to make directions to network providers to 'do, or not do, a specified thing' to protect such networks from national-security risks.

Although these powers have been in place for almost five years, a recent review by the Australian National Audit Office noted that annual reporting doesn't include any performance monitoring of the impact of the TSSR regulations.[3] Consistent processes have been developed and implemented, and there's some evidence of the regulator pursuing dialogue with entities that it believes are noncompliant. However, the most extreme enforcement powers of issuing formal directions or cancelling carrier licences haven't been used. Overall, it was assessed that 'the department has not measured whether full compliance has been achieved because it has not confirmed all entities covered by the SoCI Act and the TSSR are "compliant".'[4] Despite probably incomplete compliance by all relevant entities, the annual reports do suggest that some general positive impacts have been observed, such as improved supplier risk assessments, effective advice provided to ensure the security of 5G cloud and network function virtualisation, and interventions to ensure appropriate governance of managed service-provider arrangements.[5] This would benefit from more detailed analysis of the outcomes achieved, and whether a 'softly, softly' approach to compliance has made this more, or less, effective.

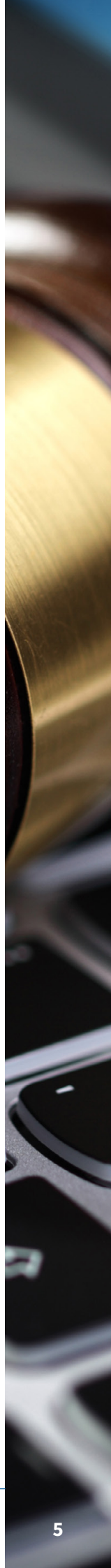


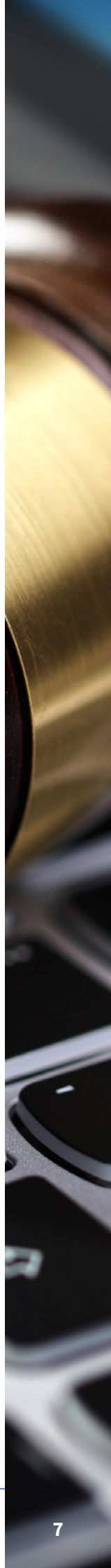
Table 1: Australian regulations with potential cybersecurity relevance

Name	Year introduced	Cyber relevance	Sector-specific?	Relevant department/ organisation	Mandatory?
Telecommunications Sector Security Reforms	2018	Yes	Telecoms	Dept. Home Affairs	Yes
Security of Critical Infrastructure Act (original)	2018	Partial (asset inventory focus)	Telecoms, transport, energy and water	Dept. Home Affairs	Yes
Security Legislation Amendment (Critical Infrastructure) Act	2021	Yes, as part of all-risks approach	Eleven specified critical infrastructure sectors	Dept. Home Affairs	Yes
Security Legislation Amendment (Critical Infrastructure Protection) Act	2022	Yes, as part of all-risks approach	Eleven specified critical infrastructure sectors	Dept. Home Affairs	Yes
CPS234	2019	Yes	Financial services	Australian Prudential Regulation Authority	Yes
Protective Security Policy Framework	2018 (major revision from previous 2014 edition)	Yes	Government departments and agencies	Attorney-General's Department	Yes
Information Security Manual	Updated monthly	Yes	No—but mainly intended for government departments and agencies	Defence	Yes for government departments and agencies
Essential Eight Maturity Guide	2017	Yes	No—but mainly intended for government departments and agencies	Defence	No
Australian Information Security Evaluation Program	2019	Yes	IT hardware and software products	Defence	In some circumstances
Hosting Certification Framework	2021	Yes	IT hosting providers	Digital Transformation Agency	No
Privacy Act	1988	No	Companies with >$3 million turnover per year, and some other organisations	Attorney-General's Department	Yes
Corporations Act	2001	No	No	Australian Securities and Investments Commission	Yes
Continuous disclosure obligations	–	No	Listed companies only	Australian Stock Exchange	Yes

Broader regulation of critical infrastructure has gone through a rapid evolution in the past five years. The *Security of Critical Infrastructure Act 2018* (SOCI Act) first came into force in July 2018 and initially covered just the telecommunications, electricity, gas, water and ports sectors, obligating around 165 operators that met certain thresholds to provide a register of key assets and ownership.[6] However, the SOCI Act has undergone significant expansion through amendments passed in two stages—the *Security Legislation Amendment (Critical Infrastructure) Act 2021* and the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022.* Those amendments have expanded the scope to cover 11 sectors, including food and groceries, health care and financial services. The number of asset classes has grown to 22, and there's now a very broad definition that includes 'any other thing' as well as a power for the responsible minister to privately declare additional assets.[7] The obligations have also been expanded to include a 'positive security obligation' to safeguard those assets, mandatory reporting of security incidents, requirements to develop and maintain a risk-management plan, and provisions for the government to be able to 'step in' to take control of an organisation's systems and networks if required to effectively respond to a cyberattack. It should be noted that the SOCI Act is generally phrased to take an 'all-risks' approach to security, but cybersecurity is a key focus area; for example, those assets designated as 'systems of national significance' have specific obligations to undertake vulnerability assessments and cybersecurity incident-response exercises.

The expansion in the definition of critical infrastructure sectors to now cover a large portion of the economy will be a challenge for regulators to implement. The government is working with stakeholders in each sector to implement principle-based rules and regulations in a phased approach. This is intended to provide flexibility to industry but will mean that regulated entities will need to make judgements that will need to be validated with the enforcement authorities to confirm compliance. Implementation is at an early stage, so it's difficult to assess how effective the regulations will be. However, initial perceptions are that the consultative phased approach to developing detailed rules should ensure that appropriate measures that improve security and encourage compliance are mandated. The risk-based approach is well chosen, although the current level appears to be set so low that it's probably less than the minimum that any well-run organisation should aim for; therefore, the legislation may be too weak to have any material impact in uplifting cybersecurity. The deadline for the first tranche of asset classes to develop risk-management plans is imminent (17 August 2023),[8] which may provide further insights and learning on how this will operate in practice.

In the financial services sector, the Australian Prudential Regulation Authority (APRA) has mandated an information security standard known as *CPS234*.[9] This aims to ensure that any APRA-regulated entity takes appropriate cyber-resilience measures, including defining roles and responsibilities, devoting appropriate resources to its information-security capabilities, implements appropriate controls and notifies APRA of any material incidents. Although the requirements are largely principles-based, from time to time APRA has issued more specific guidance about what it believes constitutes appropriate practice at that time, for example recent advice on the importance of multifactor authentication and requirements for it to be effective.[10] This is a sensible compromise involving mandating a risk-based approach, but providing guidance to help organisations understand detailed expectations, that can be updated as circumstances and technology evolve.



There are also a number of non-statutory cyber-related regulations and standards, issued by different parts of the government, that may be applicable. For example, the Attorney-General's Department issues the *Protective Security Policy Framework*, and the Australian Cyber Security Centre (ACSC) issues *the Information Security Manual* and the *Essential Eight Maturity Model*. The ACSC also runs the *Australian Information Security Evaluation Program*,[11] which uses the international Common Criteria to certify products. The Digital Transformation Agency has also issued the *Hosting Certification Framework*, which provides recommended requirements for hosting facilities. All of these are primarily intended as guidance for government systems, with potential flow-down effects on suppliers to government through relevant contractual clauses. However, they're being increasingly requested by buyers of goods and services in the private sector, which are effectively using them as a proxy for 'industry best practice' as part of their supply-chain cybersecurity checks. The existence of consistent standards helps buyers to assess the security of suppliers, but with such an 'alphabet soup' there's a risk that procurement functions that don't understand the domain well may ask for overprescriptive or inappropriate standards, given the individual circumstances of each product and service and how they're used. Suppliers would then incur unnecessary cost in proving and maintaining compliance, particularly if operating globally and also dealing with other similar standards set by other individual governments.

In our federal system, we also need to note that individual states and territories have identified cybersecurity as a critical risk and are developing and implementing their own strategies. Incentives to develop cybersecurity capability in each state can have an overall net positive impact by increasing what can be achieved at the national scale. However, competitive policies, such as an expectation (based on interpretations of legislation pertaining to physical records) that certain data needs to be stored within a state, don't provide any apparent cybersecurity benefit. While it may benefit that state's technology providers in the short term, such a competitive approach between states will simply lead to expensive, unnecessary duplication and complication of architectures and holdings of sensitive data, without any overall positive impact on national security or prosperity.

General regulations with a cybersecurity impact

Turning to more general regulations that can affect cybersecurity, the most significant example is probably the *Privacy Act 1988*, under which obligations for securing personal identifiable information from unauthorised access and use apply equally to securing that information from cyberattack. This legislation is well formulated as a principle-based approach, and there's good understanding of the obligations and how it's interpreted by the courts.

Existing company law also places general obligations on companies to manage overall risk, which includes cybersecurity risk. For example, section 180(1) of the *Corporations Act 2001* places obligations on directors of a company to act with care, skill and diligence in their decision-making. Although it hasn't been directly tested in the courts, it's generally understood that this would include prudent management of cybersecurity risk. In May 2022, the Federal Court found that RI Advice breached its obligations when it failed to have adequate risk-management systems to manage its cybersecurity risk,[12] although this was also related to its obligations as a financial services licensee.

The Australian Institute of Company Directors has highlighted cybersecurity as a crucial area for boards and has offered materials such as proposed governance principles to assist with this.[13]

However, overall, the current legislation is too high level and subject to differing interpretations; this means that at present it doesn't have a meaningful impact in setting expectations and driving behaviours.

Companies listed on the Australian Stock Exchange (ASX) are bound by *continuous disclosure requirements*, which implies a requirement to report significant cybersecurity incidents. Again, the guidance is high level and subject to interpretation, and shows how reporting obligations can have unintended consequences. This obligation has been cited as one explanation of the 'drip feed' of disclosures by Medibank in October 2022 that went from an initial statement simply stating that 'unusual network activity' had been detected to finally admitting in its sixth subsequent update that sensitive data relating to almost 10 million Australians had been stolen.[14] The impact of this drip feed was to delay wider appreciation of the potential impacts and required actions by other organisations to mitigate risk; it also gave many the impression that Medibank was deliberately downplaying the incident to protect its share price.

Lack of cohesion and its impacts

With so many different regulations, an assessment can't just consider each one individually. The overlapping framework creates significant potential for confusion and contradiction. The recent Optus data breach drew attention to the practice of telecommunications providers collecting and storing identity information on their customers. Many have suggested that such data shouldn't be collected or stored, but the practice was due to regulations requiring companies to verify customers' identities, as that's considered important in tracing the perpetrators of crimes committed using these services. There are similar obligations on financial service providers to 'know your customer' to protect against money laundering through their systems. There's a delicate balance here, as blindly removing such requirements in the name of cybersecurity would be likely to increase the incidence of other crime, such as fraud and intimidation. (Although, in this particular example, there's a potential solution using digital identity, which is touched upon below.)

Also in the telecommunications sector, the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act) has been the subject of concerns raised by local and global technology companies. It's been perceived as giving the Australian Government the right to weaken or even remove encryption of some data, thus weakening cybersecurity. Many industry stakeholders colloquially refer to the legislation as the 'anti-encryption bill'. Official communications and guidance have tried to make clear that the intention of the legislation is only to facilitate law-enforcement access to data where that doesn't compromise the general security of users of a system. However, the messaging hasn't been consistent, and no action is being taken to implement recommendations from the Parliamentary Joint Committee on Intelligence and Security[15] and the Independent National Security Legislation Monitor[16] to amend the legislation to reduce the risk of the legislation being able to be used in that way.

Another example of potential conflict is the different requirements for notification of incidents—the various regulations discussed above create different obligations in terms of expected reporting timescales and where information is to be reported to. An example is shown in Table 2.

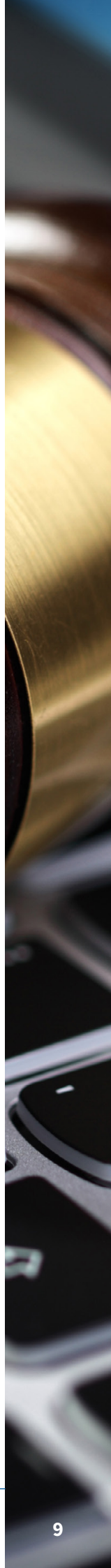


Table 2: Example incident reporting regulations in Australia

Regulation	Incident definition	Required reporting timescale
CPS 230 – op risk incident	An information security incident that: (a) materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or (b) has been notified to other regulators, either in Australia or other jurisdictions.	72 hours
CPS234 – info security incident	A material information security control weakness which the entity expects it will not be able to remediate in a timely manner.	72 hours
CPS234 – security control weakness	An incident has had, or is having, a significant impact on the availability of your asset. A significant impact is one where both the critical infrastructure asset is used in connection with the provision of essential goods and services; and the incident has materially disrupted the availability of the essential goods or services.	10 business days
SOCI Act – critical incidents	One or more acts, events or circumstances involving: unauthorised access to or modification of computer data or computer program, or unauthorised impairment of electronic communications to or from a computer, or unauthorised impairment of the availability, reliability, security or operation of computer data, a computer program or a computer.	12 hours to make an oral report, to be followed up by a written report within the next 84 hours
SOCI Act – other incidents	That has had, is having, or is likely to have, a 'relevant impact' i.e. on availability, integrity, reliability or confidentiality of the asset.	72 hours to make an oral report, to be followed up by written report within the next 48 hours
Privacy Act – eligible data breach	When the following three criteria are satisfied: • there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds • this is likely to result in serious harm to one or more individuals, and • the entity has not been able to prevent the likely risk of serious harm with remedial action.	As soon as practicable from awareness; 30-day assessment period from suspicion
ASX rules – continuous disclosure	Information 'concerning an entity' that 'a reasonable person would expect to have a material effect on the price or value of the entity's securities'.	Immediately

Source: Adapted from Gilbert & Tobin, '2023–2030 Australian Cyber Security Strategy: leading the charge', *Lexology*, 17 March 2023, online.

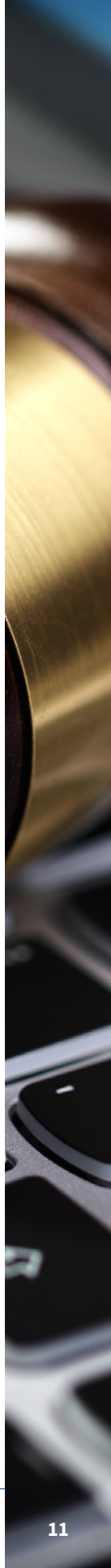
This can cause confusion and frustrate larger organisations. Some organisations seek to automate such processes to ensure that compliance with required timescales isn't impeded by their own chains of command and internal processes. Interestingly, in the period from April to December 2022, there were only 47 incidents reported under the SOCI Act provisions,[17] but, in the slightly shorter July to December 2022 period, the Office of the Australian Information Commissioner (OAIC) was notified of 222 cyber incidents, the majority of which seem to have been in critical infrastructure sectors such as financial services and health care.[18] This may reflect the different focus of the SOCI Act on availability and the OAIC on data confidentiality, and/or that the OAIC notifications scheme has been in operation for longer, so companies are better equipped to identify problems and make the relevant reports. Data on compliance with reporting timescales doesn't seem to be publicly available, but there have been no published cases of enforcement action to date for delays in response, which may suggest that the various regulators aren't enforcing strict liability for the detailed requirements where organisations are considered to have acted reasonably and in good faith.

In February 2023, the government announced the creation of a National Cyber Security Coordinator Office, and then the appointment in June 2023 of Air Marshal Darren Goldie AM CSC as the inaugural National Cyber Security Coordinator.[19] This will assist in coordinating government responses to major cyber incidents but won't immediately change regulatory obligations on private-sector organisations or address the reporting conflicts shown above.

Regulatory initiatives currently underway

A number of initiatives are already underway to update Australia's cybersecurity regulations. The *Privacy Act 1988* was recently amended to increase the fines that can be levied for data breaches,[20] while the Attorney-General's Department is conducting a more comprehensive review of the legislation that started in 2020 and is expected to continue into 2024.[21] The increased financial penalty has focused board-level attention on examining whether risks are being managed effectively, but, in the absence of modernised guidance on expectations of acceptable and unacceptable practice, this is a blunt and inaccurate instrument. Further clarity, and hence more effective impact of such regulation, will have to wait until the broader reform is concluded. It's important not to rush into regulation, but at the same time a review that takes many years runs the risk of being out of date by the time it's completed.

The *Online Safety Act 2021* is intended to tackle 'seriously harmful online content'. This is currently in the process of being implemented, and the eSafety Commissioner is directing the development of eight industry codes to cover different sectors of the online industry, noting that there is a variety of opinions on how the intended scope should be interpreted.[22] The commissioner has followed a consultative co-design process, which has included eight industry sectors being invited to propose draft codes for the commissioner to consider. In June 2023, the commissioner accepted five of those codes drafted by industry, reserved judgement on one, and for the other two has decided to develop the commission's own code, as it didn't consider the proposal drafted by the industry to be acceptable. This is an example of a co-design approach, but also shows that in this case the eSafety Commissioner acts as the final arbiter about whether or not to accept the proposed approach from the sector being regulated. It remains to be seen how those sectors in which industry's proposed code has been overruled will approach the requirements compared to those sectors for which the co-designed approach has been accepted.



The Australian Competition and Consumer Commission (ACCC) has been conducting an inquiry into digital platform services since February 2020.[23] The scope is broad and covers several economic and commercial topics, but also includes 'practices of suppliers in digital platform services markets which may result in consumer harm', which may include cybersecurity risks and impacts. The inquiry is due to be completed by May 2025 but publishes interim reports every six months. At the moment, this simply adds further uncertainty to the regulatory climate, so better clarity on the scope of any cybersecurity considerations would help drive industry investment in the right areas.

Finally, as I've noted in the introduction to this paper, the Australian Government is currently developing a new cybersecurity strategy for 2023–2030, and a number of public presentations by those leading that work have flagged that improving and/or harmonising the regulatory regime is likely to be a key focus area of the new strategy.

International examples of interest

Australia faces a variety of challenges in considering where and how to use regulation as part of its cybersecurity strategy. In considering how to approach this problem, it's interesting to look at examples of how other countries have addressed it. The Minister for Home Affairs and Minister for Cyber Security, Clare O'Neil, has said that Australia is five years behind the rest of the world on cybersecurity,[24] so what can we learn from other countries that are potentially ahead of us? This section considers the approaches taken by our AUKUS partners, as well as some relevant information from the EU and Singapore.

United States

So far, the US has taken a sector-specific approach to cybersecurity regulations. Examples include regulations such as the Health Insurance Portability and Accountability Act Security Rule, which establishes standards for the protection of electronic health information and requires covered entities to implement administrative, physical and technical safeguards, and the Defense Federal Acquisition Regulation Supplement, which imposes specific cybersecurity requirements on contractors and subcontractors of the Department of Defense. As in Australia, there's also an overlay of a patchwork of state-specific regulations such as the California Consumer Privacy Act and the New York State Department of Financial Services Cybersecurity Regulation, and various voluntary standards, of which the National Institute of Standards and Technology cybersecurity framework is the most well known and widely used. Implementation relies on extensive litigation, and the patchwork approach means that effectiveness is limited.

However, over the past 12 months, the US Government has moved to implement a range of broader regulations through executive orders that require government organisations to implement zero-trust architectures, post-quantum cryptography and a 'software bill of materials'. Those changes effectively leverage government procurement power, as government organisations pass those requirements on to their suppliers, forcing them to adapt their product and service offerings to remain eligible to bid for lucrative government contracts. Although Australian Government buying power is much smaller, this is a lever that could be better used,[25] and alignment with the US could help further magnify the impact of that buying power.

In March 2023, the US Government announced a new cybersecurity strategy that reinforces this trend, calling for a fundamental shift to move the responsibility for defending cyberspace 'away from individuals, small businesses, and local governments, and onto the organizations that are most capable and best positioned to reduce risks'.[26] This envisages regulations to hold data stewards accountable,[27] to mandate basic security of IoT (internet of things) devices, and to make producers of insecure software liable if they're shown not to have taken reasonable precautions to secure their software. Of course, it remains to be seen how much can be legislated, given split control of Congress, a hyperpartisan political climate and an established tradition of pork-barrelling that tends to bog down many major pieces of legislation.

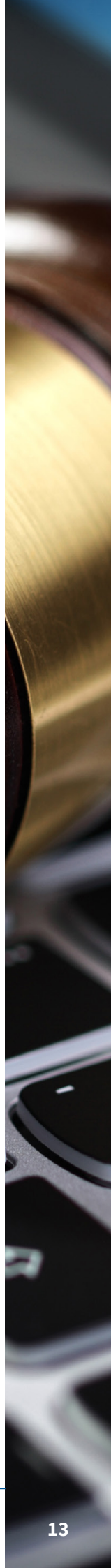
Nonetheless, Australia should consider this approach of focusing on risk management, and the transfer of risk to those best placed to manage it, in accordance with textbook recommended practice. The greater market power of the US means that Australia may have more impact by supporting the US's efforts than by seeking to act alone; however, it may have limited influence on the timescales or detailed direction. Also, choosing the biggest companies as targets for regulation also means choosing targets with strong lobbying influence and the willingness to push back against any perceived overreach by government.

United Kingdom

The UK is covered by the EU's General Data Protection Regulation (GDPR), which was adopted in 2016 and is often considered to be one of the most stringent such regulations. Although not cybersecurity-specific, it regulates the confidentiality of customer data, obliging companies to take reasonable care to prevent data breaches. The GDPR is backed by potentially eye-watering penalties—although the biggest headline numbers have been for other privacy breaches due to deliberate failure to implement internal controls on obtaining user consent and the use of data (for example, Google, Facebook and WhatsApp). The, the UK Government has fined British Airways[28] and Marriott[29] approximately GBP20m each for data breaches caused by cyber-attacks.

The UK introduced the Network & Information Systems (NIS) Regulations in May 2018, aimed at raising levels of cyber security and resilience of key systems.[30] Flowing originally from an EU directive, these include provisions at a national government level to have a framework and 'competent authority' (the NCSC in the UK) to manage cyber incidents and to cooperate with other EU Member States. They also oblige 'operators of essential services' to implement appropriate security measures to manage risks to their systems and to report cyber incidents to the government; that is, to implement preventive measures and have incident-reporting processes. The Department for Science, Innovation and Technology is responsible for the NIS Regulations. These arrangements seem to be similar to the SOCI Act approach in Australia, but less detailed, so there's probably little Australia can learn from this.

The UK Government also runs the voluntary 'Cyber Essentials' scheme that encourages organisations to adopt certain minimum standards and recognises those that do so. The standards are defined by the National Cyber Security Centre, and certification is provided by a commercial partner, the IASME Consortium.[31] This scheme appears to be well regarded, helps to modify buyer behaviours, and seems to be able to scale up certification by using a commercial partner, and hence could be a good model to follow. A recent review supports the perceived value and the positive impact on cyber behaviours but recommends some improvements to address barriers to certification.[32]



More recent regulatory initiatives in the UK have had a mixed reception. The Product Security and Telecommunications Infrastructure Act 2022 (PSTI Act)[33] and subsequent regulations were developed in close consultation with industry and appear to be well regarded. Part 1 specifies requirements for IoT security using a combination of mandatory minimum standards (compulsion) and an optional 'kitemark' that product manufacturers can display if they meet an enhanced set of requirements—intended to facilitate market signals to encourage security improvements by providing consumers with reliable and consistent information. Implementation is still at an early stage (draft regulations have been published) and the intended effective date is 29 June 2024, but this combination would be a good approach for Australia to consider.

However, the Online Safety Bill, intended to target online child sexual abuse and other cybercrime, which is currently before Parliament, has met significant resistance from many online service providers. The wording appears to be broadly drafted, and companies such as Apple,[34] Meta and Signal are concerned that it could effectively prevent end-to-end encryption, leading to reduced general cybersecurity and privacy for users. This reflects the challenge that governments face in drafting regulations, needing to make trade-offs between targeting different harms. However, this also has echoes of the debates about Australia's TOLA legislation discussed above, and again shows the need for better communication and transparency in the development and implementation of regulations.

European Union

The two most important cyber-related regulations in the EU are the GDPR and NIS directives, discussed in the UK context above. However, in recent years, the EU has continued to take an activist role in bringing in regulations, and, due to its large market power, many global companies are effectively obliged to comply in order to have access to that market. That normally results in the companies changing their global product and service offerings to benefit everyone, rather than establishing and maintaining EU-specific variants. This can provide Australia with benefits that it couldn't achieve by regulations within its own much smaller market.

More recently, as well as some reactive bans on areas of concern (for example, to address concerns over generative artificial intelligence[35]), a significant recent development has been the creation of an EU cybersecurity certification framework,[36] administered by the European Union Agency for Cybersecurity (ENISA); this will provide consistent market signalling to EU customers of products and services that meet certain standards. Again, Australia should consider mutual recognition of such certifications to benefit from the work done to define them and minimise compliance burdens on suppliers.

Singapore

Singapore is generally a smaller and more tightly regulated economy than Australia and the other examples discussed above, and hence much of what's applicable to Singapore might not be well suited to the Australian context. However, one recent development has been highly regarded by industry stakeholders: the launch of a voluntary cybersecurity certification scheme by the Cyber Security Agency in March 2022 that consists of two levels—Cyber Essentials and Cyber Trust.[37] This was developed in consultation with stakeholders and took into consideration the types of enterprises in

the country and their needs. In particular, the administrators of the Cyber Trust mark uses a risk-based approach, assessing up to 22 domains to define a preparedness tier for the organisation, depending on criteria such as governance, protective measures and resilience. In order to assist organisations in procuring IT products and services that will help them to meet their targeted preparedness tier, the government has also worked with providers to ensure clear labelling of such products and services in terms of the required measures. Such a voluntary system that aligns assessments of both buyers and sellers offers a pragmatic approach that Australia should consider.

The way forward: a new framework for defining cybersecurity regulations

As shown above, there's a complex patchwork of cyber regulations already in place in Australia and a range of approaches used overseas that the Australian Government could choose to emulate and apply. To assist with analysis of the current and potential future regulations, a framework is proposed for defining such regulations. Discussion of such a framework helps to identify the factors that should influence the choices made for each aspect and to enumerate the options currently used and those that potentially could be used.

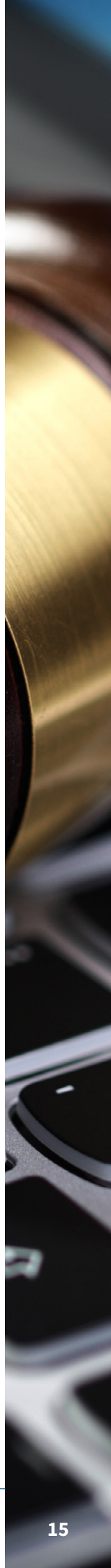
Purpose

The starting point should be to have a clear understanding of the purpose of cybersecurity regulation. We need to ask:

- What aspect of the cybersecurity problem does the regulation seek to address?
- What's the desired impact on cybersecurity from the regulation?
- Why is regulation the most appropriate solution to address this aspect of the problem and deliver the desired cybersecurity outcome?

For example, regulation may be intended to provide strategic direction to people and organisations and drive cultural change about cybersecurity. More specific approaches could seek to set a minimum baseline of security to address market failures, such as driving out lowest cost providers that don't implement a sufficient level of security. Regulations could also be used to give the market clarity about the responsibilities of different parties for security, such as the US proposals for liability for insecure software that make clear the responsibility of software developers to ensure the security of the code that they write. Another purpose of regulation could be clarifying exactly what government will and won't do, including whether particular activities that government could conduct, such as threat detection and the disruption of attackers, are intended to be regular business as usual or are only allowed in specific circumstances.

Other regulations may set a framework to enable providers to offer improved security as a competitive differentiator in a meaningful way to allow purchasers to make informed decisions. For example, this could be a common framework for security claims that allows buyers to compare offerings between providers, and to address misleading claims by providers.



Target

Regulation should be clear about whom it seeks to target and the specific behaviours that it seeks to modify. When considering a product or service being offered to end users, options for which the regulation applies could include:

- the source of supply (the manufacturer or developer of the components used to make the product or perform the service)
- the third-party integrator (a service provider who integrates the supply chain to provide the offering to the end user)
- the end user.

When making this choice, consideration should be given to which party is best placed to manage the risk, and where behaviour modification will be most effective.

Examples of source-of-supply regulation are the UK PSTI regulation to set minimum security standards for consumer IoT devices and the proposed US software developer responsibilities for secure-by-design software.[38]

Service-provider regulation would target companies such as IT managed-service providers or cybersecurity services firms. To date, there's been little direct regulation in that area, but the Singapore certification scheme is an example of introducing standardised labelling of services to inform buyers of the level of security being offered by the provider.

End-user regulation is less common, but one relevant example is the Payment Card Industry Data Security Standards, which specify how payment card information collected online needs to be secured.[39] This drives small businesses buying online services to use accredited payment gateways to ensure that they're compliant with the standard.

Finally, we shouldn't forget the Australian Government as the target of regulation. Different government departments have different responsibilities and priorities, and there are strong arguments for ensuring that they all take appropriate action to secure the citizen data that they hold and the availability of the critical services that they offer. The government also holds the national-security risk of Australian data being exposed to malicious actors and activities of foreign states—whether it's sourced from government agencies, private companies or individuals. It's often been noted that although in Australia the Privacy Act penalties have increased, and the scope of businesses covered is increasing, state and federal government bodies are exempt from the Act.

Approach

Compulsion is the most direct approach that could be used, clarifying the statutory duties of an organisation and the penalties for noncompliance. Such an approach must also consider how compliance will be enforced, including appropriate resources for the enforcement authority. Compulsion clearly has a role to play when, for example, self-regulation fails (such as the decision of the UK to introduce the PSTI Act regulations on IoT security), or simply to help companies understand their cybersecurity responsibilities and to help justify spending shareholder funds on compliance.

Encouragement is another approach. Here, organisations can choose whether or not to comply but are given incentives to do so. Examples include schemes such as mandatory labelling of products with security ratings, being given preference for government procurement if specific standards are met or clarifying the liability of software development companies if certain principles are met. Tax or other financial incentives could also be used; for example, the May 2022 Budget measure to provide a tax deduction for expenditure by small businesses on cybersecurity[40] (although in that case it was legislated so late that it's unlikely to have had any meaningful impact on buying behaviours).

Finally, government should also consider alternative approaches of facilitating, enabling, or both. This could include, for example, promoting skill development and recognition, or legal frameworks for the responsible disclosure of vulnerabilities and for incident reporting.

The government should consider a more active role in cooperation and intervention. One example would be enhancing or redesigning current government–industry threat-sharing solutions to enable the sharing of real-time threat intelligence that organisations could use to automatically detect and prevent cyberattacks. Different solutions may be needed for different purposes; for example, a platform for ACSC to 'mass broadcast' machine-readable indicators of threats and remedies to all relevant Australian entities will be different from a solution for two-way sharing of strategic threat intelligence between the key public- and private-sector players active in this sphere.

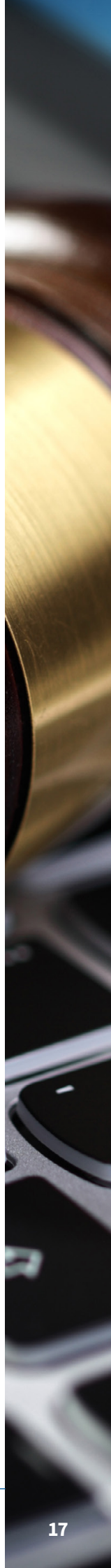
Another example is the proposed digital identity scheme,[41] which could reduce the need to collect and retain personal information to verify customers' identities, and current programs to promote diversity and resilience in 5G network infrastructure providers.[42] The Cyber Wardens program announced in the May 2023 Budget could be another example of government playing a key facilitation and enabling role,[43] although details are still awaited, and there appears to be some controversy over how the provider was selected and funds committed even before the measure was announced. An example from the past that could be revived was the action taken by the previous government to fund AustCyber—an industry growth centre to support the development of Australia's cyber industry that could provide the cybersecurity capabilities that the rest of the economy needs.

Metric or measure

Finally, regulators need to select and define one or more metrics that they seek to directly measure and control. The desired overall impact is an uplift in cybersecurity, but that's difficult or even impossible to directly target or measure. Therefore, regulation should seek to directly influence one or more direct outputs that, subject to assumptions and dependencies that will need to managed, are expected to generate outcomes that lead to this desired impact. Focused efforts will be needed to measure and evaluate those direct outputs to monitor the effectiveness of the regulation.

Regulations could be framed in terms of security outcomes, but, as any cyber professional knows, it's impossible to guarantee zero breaches, so this would need to be caveated with 'as far as is reasonably possible', which could be difficult to define and leave much open to be determined by the courts.

Risk-based approaches offer an appropriate compromise, requiring organisations to assess risk and take actions to minimise the likelihood and consequences of key risks. The SOCI Act in Australia takes this approach and is generally well regarded. However, supporting and assessing compliance can be complex and expensive, as each organisation's risk profile and tolerance will vary.



Technical compliance requirements are easier to assess, such as Essential Eight compliance, or the detailed requirements in the Hosting Certification Framework for the location of data, physical controls and so on. However, specific technical measures can reduce efficiency and flexibility, as there's usually more than one way to achieve the desired outcomes. Specifying effective technical measures requires a detailed understanding of the relevant technology; government might not necessarily have that expertise and hence may need to work with technical experts in the field, who will often be part of the organisation being regulated. Furthermore, because technology changes rapidly, it's difficult to keep such requirements up to date, and as a consequence this may stifle ongoing improvement and innovation in how capabilities are delivered to users. A compromise could be made by mandating an industry-accepted technical standard and then allowing the standard to be updated as the threat environment and technology change over time.

Other options include procedural and process requirements, such as requirements for boards to implement a cybersecurity strategy or, at a more detailed level, ensuring that an incident-response plan exists. However, going down to that level is far removed from the desired outcomes, and without managing a number of other dependencies it's unlikely that such measures alone will bring any cybersecurity uplift.

Other issues to consider

All regulatory approaches carry a risk of unwanted consequences. That can include the direct impacts of the cost of implementing the regulations and ensuring ongoing compliance, as well as indirect costs of diversion of resources and restrictions on capabilities.

There can also be third-order effects. For example, the costs of regulation could be unevenly distributed across different groups in society, potentially affecting equality and distribution. Mandatory standards may raise the cost of a product, making it less accessible to some sectors. Also, regulatory actions by the Australian Government can affect perceptions of sovereign risk and therefore the willingness of entrepreneurs and investors to operate in Australia. This was seen in the public discourse when the TOLA legislation was passed in Australia and in similar discussions today about the UK Online Safety Bill, as discussed above. Assessment of such potential effects should be part of regulatory design. The interplay with other regulations also needs to be considered; I've discussed some existing conflicts between different regulations, and any proposed new measure needs to be assessed in the context of existing measures. Ensuring that the scope of regulation is the minimum necessary to achieve the desired outcome can help to minimise those risks.

For any proposed regulatory measure, therefore, it's necessary to conduct an analysis of the expected benefits and costs compared to other options, including the 'do nothing' option. Such analysis may rely on various assumptions at the initial planning stage, but those can be tested and revised as the regulations are developed and implemented.

Conclusion and recommendations

Regulation is a vital tool that forms part of a suite of tools to improve the cybersecurity and resilience of Australia, in pursuit of the Australian Government's stated goal of becoming the most cybersecure country in the world by 2030. However, it's important to take a holistic look at what's motivating the behaviours of organisations and to consider regulation in the broadest sense—not only compulsory mandates to do or not do something, but also to use the power of incentives and 'nudges' to change behaviour to increase cybersecurity.

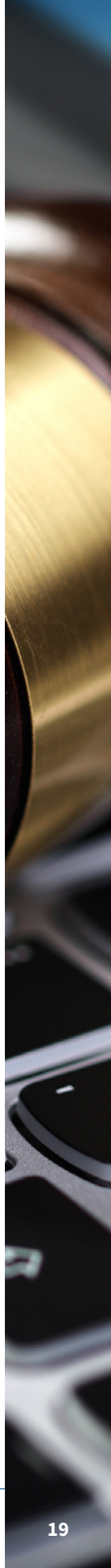
The following recommendations are proposed to the Australian Government in order to make the most effective use of regulation in an integrated cybersecurity strategy.

1. ***Use compulsion carefully and strategically*** because of the costs that compulsion imposes on organisations for compliance, and on government, which must carry out the enforcement. Mandatory measures are difficult to adapt if they're found to have unintended effects, if they're ineffective or if the technology or environment changes. Regulations could be set up such that parliamentary approval would be required, which would take time; or broad powers could be given the relevant minister to specify the details of implementation, which can then introduce uncertainty and sovereign risk for organisations. A focus on compliance can reduce incentives for organisations to do more than the bare minimum needed. Hence, although it could be appropriate to use compulsion for setting minimum 'cyber hygiene', that should be combined with other measures to encourage and facilitate organisations to go further. Compulsion will of course always have its place when other mechanisms have failed or would reasonably be expected to fail, but that must always be explicitly tested and challenged.

2. ***Measure impact***. Any new regulations that could have a cybersecurity impact should clearly define the measure or metric that the government expects the regulation to directly influence. The regulators should put in place arrangements to measure the baseline and the change after implementation.

3. ***Implement a risk-based approach***, wherever possible, for all new regulations, given that explicit cybersecurity uplift is difficult to guarantee or verify. Where that isn't feasible, technically based outputs should be used to mandate minimum expected levels of security, or otherwise there should be a mechanism, such as links to an industry-wide standard, to provide adaptability and futureproofing.

4. ***Co-design through genuine consultations and cooperation with all affected stakeholders***. This is vital in the design and implementation of any regulatory measure. Cybersecurity is a complex topic, in both technological detail and the interdependencies of multiple systems and organisations, and government alone is unlikely to have the expertise and knowledge to design the optimal approach. Measures will be effective only when technical, people and process aspects work together, and soliciting a wide range of views is the best way to test hypotheses about how regulations might work before trying to implement them.[44]



5. ***Communicate transparently with all stakeholders, including the public***, throughout the process, as this is vital to influence perceptions of the approach taken, and how constructively stakeholders respond. That communication must include providing clarity up front on the intended purpose of the regulation and how the regulation's effectiveness will be measured and ensuring that all stakeholders have access to appropriate mechanisms to put forward their point of view.

6. ***Develop regulations as an ongoing iterative process*** focused on continuous improvement. There should be regular evaluation of the implementation process, of progress towards the defined measures of success and of any unintended consequences. Appropriate feedback loops should be used to take those inputs and use them to adjust the approach as required. This will also help in futureproofing the approach.

7. ***Analyse the overlapping nature of current regulations***, including how they interact with one another, and highlight potential conflicts with other regulations at all stages. This should be conducted by the Attorney-General's Department and should include an 'all-risks' approach to ensure that a focus on cybersecurity doesn't end up increasing other security risks in the economy and society (and vice versa). Clear communication of the identified potential issues and the approach to mitigating them will be important in driving the desired behaviours.

8. ***Set an objective of regulatory simplification***. The Office of the National Cyber Security Coordinator in the Department of Home Affairs should use that objective to assess all proposed changes. A key aim of the new cybersecurity strategy developed by the department should be to reduce uncertainty about the obligations of organisations and the communication touchpoints they need to use. If a new Cybersecurity Act is to be introduced, it should replace some of the existing patchwork of legislation, not add to it, and it should be framed in a way that doesn't remove focus on other security risks.

9. ***Include consideration of the international regulatory climate and trends***. The Department of Home Affairs should explicitly include this as part of the upcoming cybersecurity strategy. This should include assessing the potential for synergies, in particular with approaches taken by like-minded allies such as those in the Quadrilateral Security Dialogue and AUKUS. That includes opportunities to learn from the experiences of others, and also to increase influence on multinational organisations, beyond what Australia can achieve on its own.

10. ***Apply Australia-specific rules only by exception***. The flip side of international regulation is the potential for conflicts and fracturing of the market if Australia sets its own bespoke regulations. Instead, the Department of Home Affairs should maximise 'equivalency' where compliance or alignment with another allied country's approach or accepted standard is considered good enough for application in Australia. That allows us to benefit from the efforts of others in defining the standard and certifying against it. It will also reduce the burden on businesses, which should reduce costs and increase innovation in the delivery of capability to Australia, and will be particularly critical in enabling the technology-sharing benefits of AUKUS and other alliances to be realised.

Notes

1 Department of Home Affairs (DHA), '2023–2030 Australian Cyber Security Strategy', Australian Government, 2022, online.

2 DHA, *Telecommunications Sector Security Reforms (TSSR) administrative guidelines*, Australian Government, April 2022, online.

3 Australian National Audit Office (ANAO), 'Administration of critical infrastructure protection policy', Australian Government, 21 June 2022, online.

4 ANAO, 'Administration of critical infrastructure protection policy', paragraph 3.34.

5 DHA, 'Appendix J: Telecommunications sector security reforms, 2021–22', in *Department of Home Affairs annual report 2021–22*, Australian Government, 2022, online.

6 'Security of Critical Infrastructure Bill 2018', Australian Parliament, 2018, online.

7 Cyber and Infrastructure Security Centre (CISC), 'Security Legislation Amendment (Critical Infrastructure) Act 2021', factsheet, DHA, Australian Government, 2021, online.

8 CISC, 'Critical Infrastructure Risk Management Program is live', news release, Australian Government, 26 May 2023, online.

9 Australian Prudential Regulation Authority (APRA), 'Prudential Standard CPS 234: Information security', Australian Government, July 2019, online.

10 APRA, 'Use of multi-factor authentication (MFA)', Australian Government, 26 May 2023, online.

11 Australian Signals Directorate, 'Australian Information Security Evaluation Program (AISEP)', Australian Government, 26 September 2022, online.

12 Australian Securities and Investments Commission, 'Court finds RI Advice failed to adequately manage cybersecurity risks', media release, Australian Government, 5 May 2022, online.

13 Australian Institute of Company Directors, 'Release of Cyber Security Governance Principles', media release, 21 October 2022, online.

14 Paul Smith, 'Disclosure questions emerge as ASX braces for wave of cyber halts', *Australian Financial Review*, 8 November 2022, online.

15 'Review of TOLA (assistance and access) regime', media release, Australian Parliament, 22 December 2021, online.

16 Independent National Security Legislation Monitor, 'Telecommunications and other Legislation Amendment (Assistance and Access) Act 2018 and related matters', Australian Government, 9 July 2020, online.

17 Ry Crozier, 'Gov sees 47 mandatory cyber incident reports in nine months', *IT News*, 14 February 2023, online.

18 Office of the Australian Information Commissioner, 'Snapshot', *Notifiable data breaches report: July to December 2022*, Australian Government, 1 March 2023, online.

19 Prime Minister, Minister for Home Affairs, Minister for Cyber Security, 'Appointment of National Cyber Security Coordinator', media release, 23 June 2023, online.

20 Mark Dreyfus, 'Parliament approves government's privacy penalty bill', media release, 28 November 2022, online.

21 Attorney-General's Department, 'Review of the *Privacy Act 1988*', Australian Government, 2022, online.

22 eSafety Commissioner, 'Industry codes and standards will protect Australians from illegal and restricted online content', Australian Government, no date, online.

23 Australian Competition and Consumer Commission, 'Digital platform services inquiry 2020–25', no date, Australian Government, online.

24 'Hacks expose Australia as years behind on cybersecurity', editorial, *Sydney Morning Herald*, 10 November 2022, online.

25 Rajiv Shah, *Working smarter, not harder*, ASPI, Canberra, 18 August 2020, online.

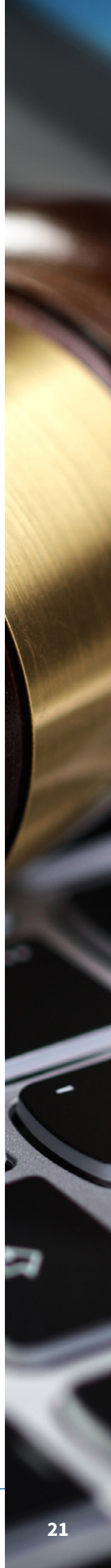
26 'Fact sheet: Biden–Harris administration announces National Cybersecurity Strategy', The White House, 2 March 2023, online.

27 Data stewards are a defined role in data governance. They have oversight and governance responsibility for specific datasets within an organisation and are responsible for enforcing policies on data usage and security.

28 RPC, 'British Airways slapped with biggest ever fine for data breach', *Lexology*, 15 January 2021, online.

29 Charlie Osborne, 'Marriott fined £18.4 million by UK watchdog over customer data breach', *ZD Net*, 2 November 2020, online.

30 National Cyber Security Centre, 'NIS introduction', UK Government, no date, online.



31 National Cyber Security Centre, 'About Cyber Essentials', UK Government, no date, online.

32 Department for Science, Innovation and Technology, 'Cyber Essentials scheme process evaluation', UK Government, 22 June 2023, online.

33 'The UK Product Security and Telecommunications Infrastructure (Product Security) regime', UK Government, 2023, online.

34 Chris Vallance, 'Apple joins opposition to encrypted message app scanning', *BBC News*, 27 June 2023, online.

35 'EU AI Act: first regulation on artificial intelligence', news release, European Parliament, 14 June 2023, online.

36 European Union Agency for Cybersecurity, 'Cybersecurity Certification Framework', no date, online.

37 CSA Singapore, 'Cybersecurity Certification Scheme', Singapore Government, no date, online.

38 Skye Witley, 'Software maker liability is elusive target of US cyber plan', *Bloomberg Law*, 3 March 2023, online.

39 'Payment Card Industry Data Security Standards', NAB, no date, online.

40 Justin Hendry, 'Small business tax breaks for cloud, cyber security grow', *IT News*, 29 March 2022, online.

41 Rajiv Shah, *The future of digital identity in Australia*, ASPI, Canberra, 17 March 2022, online.

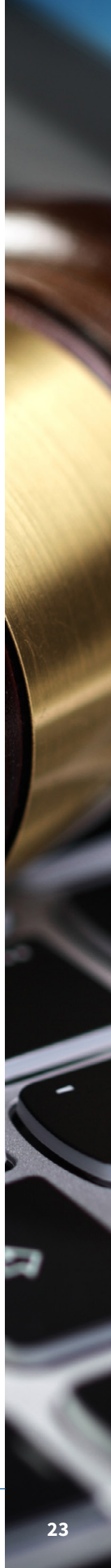
42 Ry Crozier, 'Australian government to vet 5G, 6G security in new lab', *IT News*, 18 July 2023, online.

43 Simon Crerar, 'Budget 2023: $23.4 million for small business cyber wardens program, delivered by COSBOA', *SmartCompany*, 9 May 2023, online.

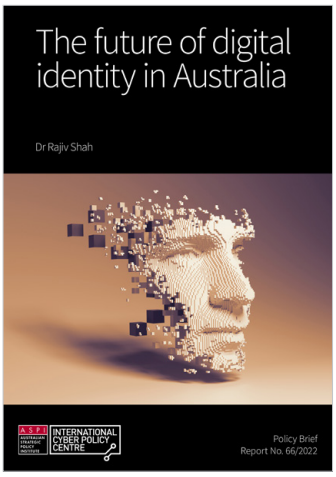
44 As a side note: however, at the whole-of-government level there's a need to co-ordinate consultation exercises. Such is the pace of change in this area that some industry associations report working on half a dozen responses to consultations at any one time.

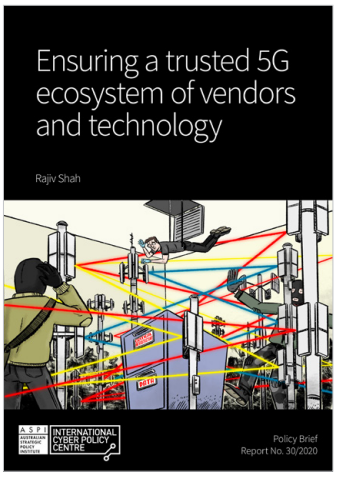
Acronyms and abbreviations

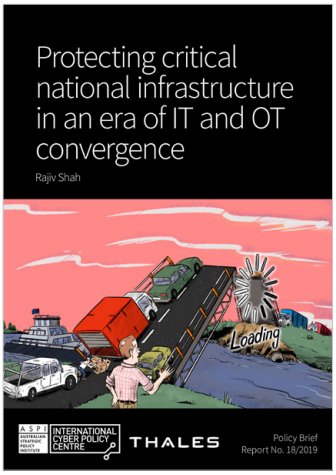
ACCC	Australian Competition and Consumer Commission
ACSC	Australian Cyber Security Centre
APRA	Australian Prudential Regulation Authority
ASX	Australian Stock Exchange
EU	European Union
GDPR	General Data Protection Regulation (EU)
IoT	internet of things
IT	information technology
NIS Regulations	Network and Information Systems Regulations (UK)
OAIC	Office of the Australian Information Commissioner
PSTI Act	*Product Security and Telecommunications Infrastructure Act 2022* (UK)
SOCI Act	*Security of Critical Infrastructure Act 2018*
TOLA Act	*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*
TSSRs	Telecommunications Sector Security Reforms

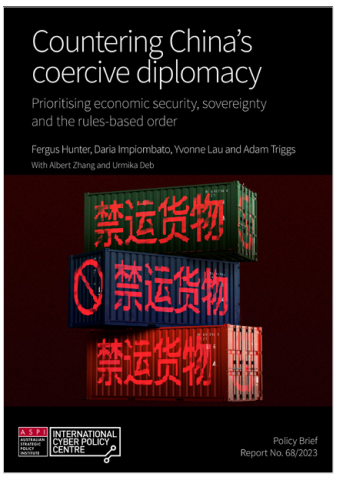


Some previous CTS publications









ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE