BCA

Business Council of Australia

2023-2030 Australian Cyber Security Strategy

April 2023

Contents

1. Overview

Cyber security is front of mind for businesses across Australia and has been for a number of years. In 2021, 95 per cent of local CEOs said cyber is a top threat to growth.[1]

Business concerns have continued to rise as the threat environment has worsened, with malicious cyber activity increasing in frequency, scale, and sophistication. It has been matched with an increasing level of focus on the part of regulators, including internationally, such as through the SEC's Cybersecurity Regulations and likely amendments in future.

Unfortunately, the risks Australia faces are not static. The Australian Cyber Security Centre's (ACSC) annual threat reports have repeatedly highlighted the evolving nature of the threats faced by Australians and Australian businesses.

Our responses must remain similarly agile. As the Minister for Cyber Security, the Hon Clare O'Neil MP has noted, Australia's 'patchwork' of approaches has not kept up.

While recent high-profile breaches have heightened concerns for Australian citizens and businesses, they have also drawn into stark relief the flaws and limitations in the current structures and systems.

A new cyber security strategy is an opportunity to ensure our systems and bureaucracies not only match the new world but keep pace with changes we know are coming.

To underpin new structures, a clear goal is needed for a refreshed cyber security strategy.

A new cyber security strategy must work towards protecting all Australians against the threats that have come with a digitised economy and society. This means having positive incentives for all stakeholders – individuals, businesses (small, medium, and large), community and not-for-profit groups, and government agencies and departments – to do the right thing.

Equally, the strategy must support Australia becoming frontier economy – a country that is diversified, competitive, and outward looking. This will be the only way Australians can get high wage, secure jobs, and a continuing improvement in the standard of living.

If Australia is going to be a top five digital economy, we must ensure there are the maximum incentives for businesses and the community to embrace digital technology, while protecting privacy and data integrity.

To get there, Australia must avoid punitive or inflexible responses to cybersecurity risks save for circumstances which demonstrate gross negligence and recklessness which meet a criminal standard of proof. Further it is important to keep a clear distinction between privacy and cybersecurity frameworks. There will be significant confusion in the Australian economy if these are somehow merged.

Responding to cyber threats must be a shared, 'team' responsibility: businesses should be seen as partners for government, along with working with the Australian community and customers. Government or regulator responses should not re-victimise organisations or individuals who are already trying to cope with a crime committed against them. Instead, government should set out a plan to construct bidirectional, timely information sharing.

In an environment where business investment as a share of GDP is at 30-year lows and capital is leaving Australia on a scale not seen since World War II, Australia can't afford to throw more sand in the wheels.

Instead, we should seize the opportunity to not just protect our existing assets and people, but also to grow a new services sector and cross-economy capability.

There are already great examples of businesses in Australia doing this. Australia should look to capitalise on their success and the recent the AUKUS defence agreement.

[1] PwC 2021 https://www.pwc.com.au/ceo-agendas/ceo-survey/2021/pwc-australia-24th-ceo-survey.pdf

But if the coming Strategy is to be credible, government needs to lead by example.

As the ACSC's *Commonwealth Cyber Security Posture 2020* report highlights, adoption of mandatory cyber standards (ASD's Top Four) remains at low levels across the Commonwealth government, with two-thirds of government agencies self-reporting as being at only an 'ad hoc' or 'developing' level of security; the lowest levels.[2] The ANAO's cyber resilience audit similarly found none of the seven agencies it selected for audit were fully effective in managing cyber security risk, and did not fully meet the mandatory requirements to implement ASD's Top Four.[3]

Since these reports, government has made substantial investments in cyber security. But most of this money is going back into government, such as supporting offensive cyber operations (such as the more than $10 billion through REDSPICE).

These are important investments, and support government improving its cyber posture.

But investment also needs to be made into measures that lift whole-of-economy cyber security, particularly for small to medium businesses and to address the chronic cyber security skills shortages facing all parts of the economy. Any new or existing programs must be properly assessed – whether they are delivering what they promised, whether the value for money is still there, and whether they continue to address contemporary problems and are flexible enough to address future problems and challenges.

Many of the questions asked in the discussion paper have been previously canvassed in recent years, including the Privacy Act Review, the consultation process for the critical infrastructure reforms, and particularly in the 2021 Strengthening Australia's *cyber security regulations and incentives* discussion paper. The BCA continues to stand by the positions set out in our responses to those consultations.

2. Key recommendations

The Business Council recommends:

1. Empowering the new national cyber security office and coordinator to help organisations that have suffered a major breach and/or cyber security incident and manage all government requests to victim organisations.
2. Government work towards establishing a 'single window' for reporting cyber incidents which efficiently inform relevant authorities and regulators. As a first step, a review should be undertaken to identify all reporting requirements organisations must comply with.
3. Government partner with the BCA on a cross-sectoral exercise regime, to help businesses and government understand their roles and obligations, and identify opportunities to improve the incident management frameworks.
4. Any reporting requirements and penalty arrangement include at least a temporary safe harbour for cyber incidents, with any reports treated as confidential, and not passed between agencies or used for regulatory investigation or enforcement action until such time as an incident has been contained and/or addressed.
5. The review of all legal provisions that require entities to retain personal information be undertaken as a matter of urgency, as set out in the final report of the Privacy Act Review.
6. Proceeding with the legislation underpinning the trusted digital identity framework as a priority and enabling it to be used as an alternative for businesses who are required by government to collect identity documents.
7. Jobs and Skills Australia (JSA) develop a specific workforce strategy for cyber security workers.

[2] ACSC 2021 https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/commonwealth-cyber-security-posture-2020
[3] ANAO 2021 https://www.anao.gov.au/work/performance-audit/cyber-security-strategies-non-corporate-commonwealth-entities

8. Government work with industry to develop a campaign to promote Australia as a top destination for global cyber security talent.
9. Developing a domestic strategy to raise cyber literacy across all society, such as advertising campaigns, public education opportunities, to ensure the Australian community is vigilant and risk aware to mitigate the risks and impacts of breaches across the economy.
10. Continuing to allow individual organisations to determine (in close collaboration with government where relevant) whether to pay ransoms.
11. Government work urgently to clarify what existing legislation and regulation means for ransom payments.
    a. In the interim, provide clarity that businesses and directors of companies will not be pursued individually for any liabilities for any cyber security event if commercially reasonable steps have been taken to ensure appropriate cyber security controls are in place (where those efforts are consistent with good industry practice).
12. Not proceeding with the inclusion of 'customer data' under the critical infrastructure regime, which will not deliver meaningful outcomes if an incident does occur.

3. Getting the structures right

Australia needs a cogent, clear cyber security strategy to ensure its systems and structures are fit to meet contemporary cyber challenges. The 'patchwork' of responses, fragmented responsibility across agencies and uncoordinated systems and process hamper Australia's capacity to respond to and mitigate cyber risks.

Before looking to establish a new 'Cyber Security Act', government needs to refresh its institutional arrangements and understand where the gaps and overlaps are, rather than layering additional legislation onto an already complex architecture.

There are quick wins that can be had from getting the structural reforms right.

3.1 Single coordinator

The government has already announced its intention to establish a new national cyber security office. The government has suggested this office will provide structure and strategy to work being done on cybersecurity risks across government, and, crucially, will be in place to manage cyber incidents in a proper, seamless way.

The coordinator will have a big task. It must be a trusted source of advice to government, the corporate, not-for-profit, community sectors and the public – akin to the Chief Health Officer during COVID.

Additionally, they must be empowered and resourced to support the fight against cyber criminals, and resolve bureaucratic battles.

As it currently stands, when businesses and other organisations fall victim to cyber-attacks, they face a slew of regulators, departments, and other government agencies all seeking information. Anecdotally, the reasons for this range from a desire to fulfill regulatory requirements, through to a desire to be seen to 'be present' and reactive to the situation to meet perceived community expectations.

Businesses want to work constructively with government agencies to meet regulatory or other information requests from government. What is needed is an approach that enables quick action, containing or stopping the criminal actors and supporting a focus on remediation and protection of citizens. As it stands, the current approach means victims spend too much time discharging reporting requirements and navigating red tape, or having to address criticisms being directed through the media – which does not promote a partnership approach with government.

The coordinator must be empowered to assist organisations that have suffered a breach or significant cyber security incident, and actively manage other government agencies who, though well-meaning, ultimately hinder the overall response.

The quick establishment of the coordinator is a measure we strongly support. But it must be backed in by government with two additional measures: an appropriate exercising regime to ensure the overall response mechanisms across the economy are match fit, and an appropriate and sensible 'single window' for reporting with clear process and effective, timely engagement and communication.

3.2 Exercises

The government has announced it will be undertaking exercises with specific sectors across the economy, commencing with banking and finance. These should not be used to identify opportunities for punitive measures if participants in exercises find vulnerabilities or issues. Instead, these should be an opportunity to identify lessons and principles of mitigation that can be shared across government and organisations to improve cyber resilience. Fundamentally, the exercise should be targeted towards ensuring improved communication between government and businesses.

We support government continuing to take this forward, in close consultation with all sectors – not just as participants, but also through the design and development of scenarios and post-exercise review. Exercises must be done in partnership with businesses.

Any exercises need to deliver not only practical lessons for how organisations should aim to respond and engage with government, but also identify any shortcomings or pitfalls in the current structures. This will be critical if the cyber coordinator is to be successful: the coordinator must have a focus on continually improving and updating the response frameworks.

We recommend the government partner with the BCA on a cross-sectoral exercise regime, to help businesses and government understand their roles and obligations and identify opportunities to improve cyber governance and coordination frameworks.

The key objective of the initial set of exercises will be to flush out the many and varied reporting requirements faced by businesses across the economy when a cyber incident occurs to ensure the system works effectively to deliver outcomes, rather than be caught up in a red tape reporting system that does not add value.

3.3 Single reporting window

As it currently stands, there is a 'forest' of reporting requirements businesses and other organisations must comply with, each with varying timeframes and requirements.

These requirements stem from a range of regulatory and quasi-regulatory government agencies, such as the Security of Critical Infrastructure Act, APRA requirements, the Notifiable Data Breaches Scheme, among many others. This is on top of additional requirements for publicly listed companies, such as ASX disclosure requirements. Potential additional reporting requirements have also been raised, including for ransom demands, and small businesses that could possibly be brought into the scope of the Privacy Act.

This complexity is highly problematic. Businesses have reported responding to information requests from upwards of 30 different government agencies for a single incident on an "urgent" basis. This is not helpful: as noted earlier, businesses need to be focused on protecting citizens and customers, not filling out forms.

Simplification is critical.

What is required is a single reporting window for incidents, which allows businesses to discharge their reporting requirements for as many agencies as possible through a single point, while working in collaboration with the newly established cyber coordinator.

This will not be a simple endeavour: the wide array of reporting requirements businesses face are baked into legislative and regulatory regimes. An early start will be vital: government must conduct an urgent review of the various agencies and regulators that have investigatory or information request powers, or which are likely to be involved in any cyber incidents to rationalise and streamline the requirements so that the reporting of critical information to the most relevant and effective agencies is prioritised.

4. What works

Positive settings will help Australian businesses get from where we are today to where we need to be.

Businesses – like all organisations in Australia – want to protect themselves and their customers. To help with this, government needs to put the right settings in place – like better information sharing, reforming legislative requirements for what businesses are required to hold, and pushing ahead with long overdue legislation on digital identity. An environment that encourages businesses to look for and disclose major breaches will be vital Additionally, to encourage adoption and investment in the cybersecurity strategy, governments must consider the implementation of appropriate rebates and tax deductions to enable small to medium businesses to support and maintain the strategy.

4.1 Better information sharing

Beyond reporting of specific incidents (discussed above), large-scale and quick information sharing arrangements will be vital.

Part of building greater trust and confidence in how businesses work with government requires greater information sharing. Informal CISO networks already complement formal government initiatives (eg ACSC's CTIS, or the reinvigorated Trusted Information Sharing Network).

Responding to cyber threats is not an area of competition for businesses in Australia. Government can play a critical role in facilitating the sharing of actionable information across the economy, such as technical details like indicators of compromise or signature files.

This is compromised where there are low levels of trust in information sharing arrangements. If there is a belief the information shared with government is being passed to regulators to undertake investigations for the purpose of enforcement actions, or there is a risk information shared will be used publicly to "name and shame" victims of crime, it hampers information sharing.

All 'naming and shaming' does in this context is compound harm to victims of crime. Any reporting scheme needs to recognise that individuals and organisations subjected to cyber incidents are victims, and they should not be re-victimised or subject to onerous or punitive requirements,

Organisations must also have confidence information provided early in an incident will not be used against them by regulators, who may not have the full context about information that has been shared. If businesses are required to 'vet' all information shared with government to ensure it cannot be misinterpreted by the plethora of existing regulators and government agencies, it will significantly impede disclosure and sharing of threat information.

Information sharing needs to be bi-directional and timely. As it stands, businesses find that information sharing is largely one-way, with the insights provided to government not matched with actionable intelligence being shared in return. Where information is shared by government, it can be days or even weeks after existing CISO networks have already been aware.

To resolve these issues, and lift both the engagement and trust in information sharing arrangements, any information sharing arrangements should explicitly only be used to support:

- law enforcement agencies in detecting, stopping and potentially prosecuting criminal activity that caused a breach or significant cyber incident,
- defence agencies to develop protections against broader and systemic cyber threats,
- assessment agencies to identify and report general patterns and trends so government agencies and the private sector can more effectively address cyber-crime risks and build business resilience to future threats and incursions, and
- the business community and other organisations to understand the technical indicators of compromise or quickly patch or update systems to prevent further compromises.

How any reported information is used needs to be carefully developed. Preserving the confidentiality and anonymity of reporting entities will be key: when the information is accessed or shared more broadly it must be de-identified, and strongly adhere to the well-established principle of need to know.

This will prevent adverse outcomes, such as the information sharing powers provided for in the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022*. This Bill - ostensibly intended to enhance Australian's privacy and prevent unauthorised transfers – instead created the perverse situation where private and confidential information is allowed to wash throughout government and to foreign governments with little to no controls or governance.

4.2 Reforming what businesses need to collect

The final report of the Privacy Act Review recommends a review be undertaken of "all legal provisions that require retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information" (proposal 21.6 of the Review report).

As noted in our submission to the Attorney-General's Department, the Business Council strongly supports this recommendation. This should be progressed as a matter of urgency and well before any steps are taken to change the current privacy laws.

Businesses and other organisations are required to hold substantial volumes of information by a wide range of regulations set by all layers of government. To help lift cyber security outcomes across Australia, enabling businesses to minimise the amount of data they are required to collect and hold will be critical.

What is needed is clarity from government about its expectations for the regulatory requirements to collect and hold information about Australians. Many of these laws have been in place for decades, often without review or modernisation to reflect new technologies. The complex web of data retention laws have been put in place by both the Commonwealth and state/territory governments, and apply across different sectors in Australia. They require certain information to be kept for 2 years, 5 years, 7 years and even 10 years in some cases – and potentially even longer. Consequently, there is a tendency for regulated entities to keep personal and other information for the longest prescribed period to ensure they meet legislative requirements.

Once clarity on retention is provided, organisations should be enabled to determine the other legitimate business purposes (many of which would be expected by customers) for which they may need to hold information. For instance, personal information may need to be held for longer periods to manage customer complaints on product performance or service standards. Businesses may also choose to retain information which could become subject to dispute of a core part of our business (e.g. transactions, supplier contractual arrangements), or to manage the risk of historical employee complaints, disputes and litigation.

If an organisation destroys or de-identifies that information after this assessment, they must not be penalised by regulators for not continuing to hold that personal information. For this reason, it will be critical that regulators are consulted as part of the review.

However, there are legitimate public policy reasons for businesses to be able to safely verify that people are who they say they are. This can be an important measure against financial crimes or national security concerns, and enables businesses to offer services knowing a customer is real and/or legitimate.

For this reason, it is critical government establish a secure and resilient digital identity system for Australia and allow it to be used in place of handling and storing identity documents.

4.3 Rolling out digital identity

Australians currently have little choice but to use documents like passports and driver's licences to establish their identity.

Government must accelerate the long-running digital identity work, to provide businesses a way to positively identify an individual without requiring the collection of these types of personally identifiable information. This could also encourage and support innovation in privacy enhancing technologies that allows sensitive information to be computed but not handled, and ensure citizens have better tools to help them manage and control their data sharing with businesses and government.

The legislation underpinning a trusted digital identity framework must be progressed as a priority.

While this has been an item for discussion at the Data and Digital Ministers' Meeting, this cannot be left to wallow in the quagmire of jurisdictional bureaucracy.

Key to ensure this is a success will be ensuring businesses are able to use the system to verify the identity of Australians where regulation requires them to.

This will not be a simple task: requirements to collect or verify identity are part of a wide range of legislation, regulations and best practices across a range of industries and at varying levels of government. But Australia cannot delay if we want to protect individuals.

4.4 Addressing skills shortages

One of the main constraining factors for improved cyber security outcomes across Australia is a skills shortage of cyber security professionals.

As it currently stands, there are not enough workers with the right digital skills. Worse, we risk being left behind by global competitors. Australia lags countries like the United States and Singapore in demand for cutting-edge digital skills – particularly in cyber.[4]

To ensure Australia takes a sensible and coordinated approach to filling these skills needs, we recommend Jobs and Skills Australia (JSA) be tasked with developing a specific workforce strategy for cyber security workers. This could include targeting university and fee-free TAFE places at these kinds of high demand priority areas.

This needs to inform how Australia can attract more international cyber talent. This brings fresh skills and ideas in Australia, raises supply of cyber workers, and exposes existing Australian workers to global best practice. Beyond the recently announced reforms to the migration system, this means promoting Australia as a destination for global cyber talent.

There are other quick, no-regret wins Australia can also pursue now.

Support must be provided for industry-led skills programs that seek to upskill or retrain existing workers in Australia with 'job ready' skills and industry placements, to enable them to move into cyber security careers, or lift their cyber capabilities. Further incentives should be provided in our schools and tertiary institutions to develop programmes and training for skills development throughout the education system so that Australia in time is able to supply expertise from within its own economy.

[4] https://www.nationalskillscommission.gov.au/sites/default/files/2022-03/ABS%20Paper%20-%20Digital%20Skills.pdf page 23

Further, as society and workplaces evolve in response to technological change, providing all Australians with foundational digital skills will be vital, including for cyber security.

We need to look beyond training a minority of cyber security professionals and consider ways to lift the cyber skills of our entire workforce and populace, including through awareness campaigns. Basic cyber skills should be a mandatory component in the syllabus for Australia's educational institutions. To aid in this, governments should consider providing guaranteed funding support for foundational skills, including in digital and cyber literacy, delivered through micro-credentialling. This will be particularly important for those seeking a career in cybersecurity or related fields.

5. What doesn't work

There are things we know don't work, or where the costs just won't be worthwhile.

A largely punitive approach to cyber security does nothing to protect Australians as it ignores threat actors that are highly sophisticated, persistent and organised (in many cases sponsored by nation-states). Businesses are required to take cyber security seriously from existing obligations in existing legislation, including corporate and privacy law.

Negative incentives will not meaningfully shift the dial for Australia and Australians unless they are balanced with incentives to 'do the right thing'. They must also deliver meaningful benefit to the economy or society, greater than any costs they introduce.

5.1 Ransomware payment bans

The discussion paper asks whether a strict prohibition of payments would be appropriate. This would not be helpful. Many businesses already have policies against paying ransoms.

While the paper does not discuss the logic of any ransomware payments ban, it is likely that underlying logic is that it makes Australia a less attractive target for criminal groups if payments are more difficult to extract.

It is not apparent that this approach has worked in any jurisdiction, nor does it acknowledge the threat actors' motivations or evolving 'ransom' techniques (including 'triple extortion' approaches that are becoming increasingly common). Instead, a ban is likely to see actors 'raise the stakes' – looking to take more violent, dangerous, or harmful attacks to secure a payment.

A ban on payments may theoretically improve cyber security outcomes for Australia by reducing the prospect of Australian businesses being deliberately targeted. But there are serious instances where flexibility to make payments is necessary – such as where there is a threat to life, infrastructure, the functioning of the economy, or individual businesses may be otherwise forced to close (resulting in loss and damage including job losses), among other potentially catastrophic scenarios.

Where this flexibility or safe harbour is provided in these instances, it will likely motivate threat actors to target those sectors. Perversely, this will just make those sectors a more attractive target, which would run against the policy intent of reducing the attractiveness of Australia as a target.

Reducing the attractiveness of Australia as a target for ransomware must be weighed against other public policy outcomes, such as having safe workplaces or respecting Australia's privacy (where a ransom is demanded to prevent publication of files).

Further, many ransomware incidents are not all highly targeted operations, but instead may rely on a 'spray and pray' approach, particularly those affecting smaller organisations or individuals.

Given this, it is difficult to see how a ban could be reasonably enforced: the government may wish to consider whether it is comfortable pursuing civil penalties against (or having the AFP pursue) an individual who paid $50 to regain access to their family photos.

Whether to pay should be left to individual organisations to determine (in close collaboration with government). As it stands, businesses do not take these decisions lightly. These decisions involve senior management and Board oversight, and involve a wide range of considerations, including operational resilience, reputation and business risk, and the advise of government partners.

5.2 New director's duties and clarity on legislative requirements

Clarity needs to be provided about existing obligations and how to best deliver high quality cyber security governance and risk management.

The discussion paper asks whether explicit director's duties should be imposed for cyber security. It is well accepted that existing duties already extend to cyber security risks. The problems with adding a new duty are well-rehearsed, as they have been addressed in previous consultation processes (such as the previous consultation on cyber security regulation and incentives, the outcomes of which were never released).

Fundamentally, we agree with the problem the paper identifies – a lack of clarity for all organisations (businesses and others) about how best to arrange themselves against cyber threats. But the solution is not in imposing new duties for directors.

Businesses face a range of challenges in determining the best approach to deflecting or mitigating cyberattacks (such as ransomware). This includes (but is not limited to):

- Breaches of director duties to act in the best interests of the company, or potential conflicts with fiduciary duties (where the most commercially practical approach may be to pay the ransom)
- Class actions by shareholders where a response is alleged to have had a material adverse impact on the company
- Exposure to 'instruments of crime' provisions of the Commonwealth Criminal Code
- Exposure to liability under anti-money laundering laws
- Exposure to liability under counter-terrorism financing laws
- Exposure to liability under sanctions laws, and
- A potential new 'direct right of action' or statutory tort for serious invasions of privacy, being considered through the Privacy Act Review.

Directors and officers may also face additional challenges, such as director's liability insurance (which may not cover ransomware incidents).

The Business Council supports directors and officers taking responsibility for the businesses they oversee, including appropriately managing risks in a way that best supports and enhances the business for stakeholders. However, even with the best efforts of directors, officers and employees, there is always the probability that cyber security risks will materialise. It is impossible to achieve zero cyber risk.

This creates an impossible situation for businesses, who may face legal challenge even where they have made reasonable efforts to mitigate against cyber security risks. The request for advice on how to approach a ransomware or other cyber incident may need to come quickly, in a complex, evolving, and relatively novel domain without substantial precedents, and which is likely to continue to escalate. This type of environment does not encourage disclosure.

When responding to ransomware incidents, there may also be ambiguity for directors and businesses within existing legislative requirements. These include the 'instruments of crime' provisions within the Criminal Code Act, requirements under the Privacy Act, anti-money laundering/counter-terrorism financing and Know Your Customer requirements, as well as the applicability of payments made in currencies apart from Australian dollars.

This has been compounded with recent moves by insurers to withdraw capacity and increase premiums. Moreover, if changes are introduced that are substantially different to comparable jurisdictions, it will make it challenging for underwriters based overseas to understand our position, further challenging insurance markets.

To address this, the government should also work urgently to clarify what existing legislation and regulation means for ransomware payments.

In the interim, we recommend the government provides clarity that businesses and Directors will not be pursued for any liabilities for any cyber security event if commercially reasonable steps have been taken to ensure appropriate cyber security controls in place (where such efforts are consistent with good industry practice).

Instead, government should work with businesses to develop and promote best practice guidance. If government thinks businesses are not meeting the mark on cyber security guidance, it needs to first work with businesses to help determine what 'good' looks like, and help businesses operationalise these requirements. This should be particularly focused on supporting SMEs, given they are less likely to have the skills or investment levels needs to meet and sustain these requirements.

It also needs to avoid becoming a 'tick the box' compliance exercise. Compliance does not equate to security, particularly against cyber threats, which are dynamic and constantly evolving.

5.3 Adding consumer data to critical infrastructure regimes

Finally, the paper proposes expanding the definition of 'critical assets' under the *Security of Critical Infrastructure Act* (SOCI Act) to capture 'customer data' and 'systems'. We understand this is intended to capture all customer data sets, regardless of whether they are currently in any of the 11 critical infrastructure sectors, and where the data sets hold 'sensitive' information (eg passport or drivers licence numbers). This is intended to ensure the powers (like the highly controversial and much opposed step-in powers) under the critical infrastructure act can extend to major data breaches.

We do not support this proposal.

There are current laws and proposed amendments to the Privacy Act which make this unnecessary. Additionally, it will introduce significant confusion as to which regulator operates in what sector and how the different layers of legislation apply.

It would undercut the intention of the recently reformed SOCI Act, not achieve meaningful outcomes when a data breach or significant cyber security incident does occur, and have serious negative consequences more broadly across the economy.

The SOCI Act is intended to manage threats to Australia's critical infrastructure. These are threats to Australia's social or economic wellbeing, or to the ability to conduct national defence and ensure national security. Extending the Act to arbitrarily capture this additional 'asset' would stretch the definition of 'critical infrastructure' to render it effectively meaningless.

Moreover, it is not clear how the powers under the SOCI Act would be helpful in the event of a major data breach or significant cyber security incident affecting consumer data. The government previously indicated that it expected that the 'government assistance measures' set up under the SOCI Act would only be used as a 'last resort' and only in the most critical of circumstances, where an entity was unable or unwilling to act against a cyberattack that would threaten Australia's core national interests.

It is challenging to see how a major data breach of customer data – outside of one taking place against a government body, which are not captured under the SOCI Act – would meet any of the thresholds set by government to determine 'critical infrastructure' or for the government assistance measures.

What it will do, however, is make Australia an even more challenging place to invest or do business. The SOCI Act's definition of a 'critical infrastructure asset' has important flow-on implications: one of which is for foreign investment. Under the Foreign Acquisitions and Takeovers Act 1975 (which governs the work of the Foreign

Investment Review Board (FIRBs), the threshold test to determine a 'national security business' is defined as a 'business that is a responsible entity for [a critical infrastructure] asset' – with a direct reference to the SOCI Act. Effectively, any entity responsible for a 'critical infrastructure asset' under the SOCI Act is a 'national security business', and subject to a wide range of additional requirements for investment purposes, including requiring additional approvals to start or acquire an interest in any national security businesses.

By including 'customer data' as a critical infrastructure asset, vast swathes of the economy will suddenly be brought under the FATA regime. This will clog up the foreign investment regime, which is already cripplingly slow. At a time when Australia is exporting capital on a scale not seen since World War II, it would be catastrophic to introduce additional unnecessary hurdles for investment.

It would potentially expose businesses across the economy – large and small – to comply with the complex regulatory requirements intended to protect the most sensitive systems in Australia.

BUSINESS COUNCIL OF AUSTRALIA

42/120 Collins Street Melbourne 3000 T 03 8664 2664 F 03 8664 2666 www.bca.com.au